

# 高效安全的无证书密钥协商方案<sup>\*</sup>

朱志馨, 董晓蕾

(上海交通大学 计算机科学与工程系, 上海 200240)

**摘 要:** 在网络信息安全领域, 服务器与客户机之间的密钥协商显得非常必要。无证书公钥密码是为了克服基于身份密码的密钥托管性质提出来的, 它结合了传统公钥证书密码体系和基于身份的公钥体系的优点。应用椭圆曲线的配对运算, 提出了一个两方的无证书密钥协商协议, 其中每一方只需计算一个配对, 并证明了它在 ECK 模型下的安全性。与其他无证书密钥协商协议相比, 安全性和效率都更好。

**关键词:** 密钥协商; 无证书公钥密码; 双线性配对

**中图分类号:** TP309      **文献标志码:** A      **文章编号:** 1001-3695(2009)12-4787-03

**doi:**10.3969/j.issn.1001-3695.2009.12.110

## Efficient and secure certificateless key agreement protocol

ZHU Zhi-xin, DONG Xiao-lei

(Dept. of Computer Science & Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

**Abstract:** In the area of network information security, key agreement is essential between servers and clients. To overcome the key escrow property of identity-based cryptography, proposed certificateless public key cryptography, it combined the advantages of the traditional PKI and the identity-based cryptography. This paper proposed a new certificateless two-party key agreement protocol using pairing operation in elliptic curves, it only required each party to compute one pairing. Proved its security in ECK(extended Canetti-Krawczyk) model. Compared with existing certificateless protocols, the newly proposed key agreement protocol has better security and efficiency.

**Key words:** key agreement; certificateless public key cryptography; bilinear pairing

密钥协商是网络信息安全领域非常重要的安全协议。Al-Riyami 等人<sup>[1]</sup>提出了无证书公钥的概念, 介于传统的证书公钥密码体系和基于身份的公钥体系之间, 它既不需要证书, 也不存在基于身份的密钥托管问题, 所以引起众多的注意, 但已有的无证书密钥协商协议都没有提供安全性证明。LaMacchia 等人<sup>[2]</sup>提出了扩展 Canetti-Krawczyk (ECK) 模型, 是目前最新最强的安全模型, 能捕获更多的攻击行为。本文应用椭圆曲线的配对运算, 提出了一种高效的两方的无证书公钥体系下的密钥协商协议, 证明了它在 ECK 模型下的安全性, 并对其安全属性作了分析, 能满足所有期望的安全属性。

### 1 技术背景

#### 1.1 无证书密钥协商的研究现状

Al-Riyami 和 Paterson (AP)<sup>[1]</sup>在 2003 年亚密会议上最早提出了无证书公钥密码的概念, 来解决身份基密钥托管的局限性, 它不需要证书, 是介于基于身份的密码与传统公钥密码之间的体系; 并提出了一个无证书密钥交换协议。AP 的协议计算量比较大, 要求协议的每方计算四个双线性配对。Mandt<sup>[3]</sup>对其进行了改进, 每方需要计算两个配对, 但是安全性分析存在漏洞, 其协议不能抵抗密钥妥协伪装 (KCI) 攻击。其他已有的无证书密钥交换协议也均未提供形式化的安全性证明, 安全性方面的考虑都是对攻击者类型的分析和安全属性方面启发式的分析。

#### 1.2 密钥协商协议的安全属性

为了抵抗各种攻击, 密钥协商协议需要拥有下面的安全属性<sup>[3,4]</sup>:

a) 已知会话密钥安全。每次协议的运行产生一个惟一的秘密会话密钥。敌手知道了一个会话密钥不能恢复以前或者将来的会话数据。

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) 密钥妥协伪装 (KCI) 安全。如果 A 的长期私钥被攻破了, 攻击者可以伪装成 A, 但是不能对 A 伪装成其他实体。

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

#### 1.3 椭圆曲线上的双线性映射

$G_1$  和  $G_2$  都是  $q$  阶群,  $q$  是素数,  $G_1$  是加法群,  $G_2$  是乘法群,  $P$  是  $G_1$  的一个生成元。  $e$  是一个配对:  $e: G_1 \times G_1 \rightarrow G_2$ , 并且满足以下三条性质:

a) 双线性。给定任意  $P, Q, R \in G_1$ , 有

$$e(P, Q + R) = e(P, Q) \cdot e(P, R)$$

$$e(P + Q, R) = e(P, R) \cdot e(Q, R)$$

因此, 给定任意  $a, b \in \mathbb{Z}_q$ , 有

**收稿日期:** 2009-02-28; **修回日期:** 2009-04-18      **基金项目:** 国家自然科学基金资助项目 (60673079); 国家“863”计划资助项目 (2006AA01Z424)

**作者简介:** 朱志馨 (1986-), 女, 福建龙海人, 硕士研究生, 主要研究方向为公钥密码与信息安全 (xmuzzx@gmail.com); 董晓蕾, 女, 副教授, 博士, 主要研究方向为数论密码、信息安全和可信计算等。

$$e(aP,bQ)=e(P,Q)^{ab}=e(abP,Q)=e(P,abQ)。$$

b)非退化性。 $e(P,P) \neq 1。$

c)可计算性。存在有效算法可以计算  $e(P,Q)$ 。其中: $P,Q \in G_1。$

(a) 计算双线性 Diffie-Hellman 问题(CBDH)。给定  $(P,xP,yP,zP) \in G_1。$  其中  $x,y,z \in Z_q^*,$  计算  $W=e(P,P)^{xyz} \in G_2。$

(b)判定双线性 Diffie-Hellman 问题(DBDH)。给定  $(P,xP,yP,zP) \in G_1。$  其中  $x,y,z \in Z_q^*,$  判断  $W$  是否等于  $e(P,P)^{xyz}。$

(c)Gap 双线性 Diffie-Hellman 问题(GBDH)。给定 DBDH 预言机,解决 CBDH 问题。

上述问题都被认为是困难问题,即不存在多项式时间算法,能以不可忽略的概率解决该问题。

本文提出的密钥协商方案的安全性归约到 GBDH 问题。

1.4 ECK 模型

LaMacchia 等人<sup>[2]</sup>提出的扩展 Canetti-Krawczyk (ECK) 模型与其他模型最大的不同之处在于允许泄露临时私钥信息,能够捕获更多的攻击行为。

在 ECK 游戏中,攻击者 E 可以作如下询问:

a)Send(A,B,m)。作为 B 发送一个消息给 A。返回 A 对这个消息的回应。

b)Long-term key reveal(A)。泄露用户 A 的长期私钥。

c)Ephemeral key reveal(sid)。泄露会话 sid 的一个临时私钥。Sid 用(A,B,n)表示,指 A 与 B 的第 n 次会话。

d)Reveal(sid)。泄露会话 sid 的会话密钥。

在游戏的某一刻,攻击者 E 选择一个已完成的会话 sid,发出询问 test(sid)并得到挑战值 C。E 在 test 询问后可以继续作其他的询问。游戏在 E 作询问 Guess(b')时终止。游戏对这两个询问的回应如下:

(a)Test(sid)。随机选取  $b \in \{0,1\}。$  如果  $b=1,$  令  $C=$  reveal(sid),否则 C 为随机数。返回 C。

(b)Guess(b')。如果  $b'=b,$  返回 1,否则返回 0。

E 如果能对新鲜的会话作出正确猜测,就赢得了游戏。一个 A 与 B 之间的新鲜会话是指,在这个会话中,E 并不都知道 A 的长期私钥和短期私钥,或者 B 的长期私钥和短期私钥。

(c)ECK 安全性。在协议 X 下,如果没有攻击者能在多项式时间内,以不可忽略的概率赢得如上所述的 ECK 游戏,那么协议 X 是 ECK 安全的。

2 提出的新密钥协商方案

本文提出了一个基于无证书公钥体系的密钥协商方案,能实现通信实体之间的快速密钥协商。

参数说明:协议包含三个实体,通信双方 A、B 和密钥生成中心(KGC)。KGC 的公开参数为  $params = \langle G_1, G_2, e, P, P_0, H_1 \rangle。$  其中: $G_1, G_2, e, P$  的含义与 1.2 节相同, $P_0 = sP, s$  是 KGC 的主密钥, $H_1$  是一个哈希函数  $H_1: \{0,1\}^* \rightarrow G_1。$  KGC 给在它的域中的每个实体颁发部分私钥,给 A 分发  $D_A = sQ_A。$  其中: $Q_A = H_1(ID_A) \in G_1,$   $ID_A$  是实体 A 的惟一标志。A 选择一个秘密参数  $x_A \in Z_q^*,$  完整的私钥为  $S_A = \langle D_A, x_A \rangle。$  A 的公钥为  $P_A = x_A P \in G_1。$  实体 B 也类似。

基于无证书公钥体系的密钥协商新方案如下:

A 选择一个随机临时私钥  $a \in Z_q^*,$  发送  $W_A = aQ_A, T_A = aP, P_A$  给 B。B 收到信息后,也选择一个随机临时私钥  $b \in Z_q^*,$  发送  $W_B = aQ_B, T_B = bP, P_B$  给 A。记会话副本  $PT = (W_A, T_A, W_B, T_B)。$

A

B

$a \in Z_q^*$  $b \in Z_q^*$

$W_A, T_A, P_A$  $W_B, T_B, P_B$

$K_{AB} = e(D_A, W_B + aQ_B) K_{BA} = e(W_A + bQ_A, D_B)$

$K = K_{AB} = K_{BA} = e(Q_A, Q_B)^{e(a,b)}$

$FK = H(K, abP, x_A x_B P, A, B, PT)$

在交换信息之后, A 先验证  $W_B, T_B, P_B \in G_1,$  然后计算  $K_{AB} = e(D_A, W_B + aQ_B),$  会话密钥为  $FK_A = H(K_{AB}, aT_B, x_A P_B, A, B, PT)。$

同时, B 也验证  $W_A, T_A, P_A \in G_1,$  计算  $K_{BA} = e(W_A, bQ_A, D_B),$  会话密钥为  $FK_B = H(K_{BA}, bT_A, x_B P_A, A, B, PT)。$  可以验证 A、B 生成的会话密钥是一致的, 因为  $aT_B = abP = bT_A,$  并且  $x_A P_B = x_A x_B P = x_B P_A,$  因此它们的共享相同的会话密钥为  $FK = FK_A = FK_B = H(K, abP, x_A x_B P, A, B, PT)。$  其中  $\langle K, abP, x_A x_B P \rangle。$  这部分的安全性保证只有通信双方才能计算出。在密钥生成串中包含身份是防止未知密钥共享攻击的一般方法, 包含会话副本则是为了保证不匹配的会话生成不同的会话密钥。

3 新方案分析

3.1 安全性证明

借鉴 Kudla<sup>[5]</sup>在模块化证明中使用的某些证明技巧, 证明新方案的 ECK 模型是安全的, 假设 GBDH 问题在  $\langle G_1, G_2, e \rangle$  下是困难的,  $H_1$  和  $H$  是随机预言器。

证: 假设存在攻击者 E, 能以不可忽略的优势  $\eta(l)$  赢得 ECK 游戏( $l$  是安全参数), 对  $H_1$  随机预言机最多询问  $\mu_1$  次, 对  $H_2$  随机预言机最多询问  $\mu_2$  次, 相同两个参与者的会话最多初始化  $\mu_k$  个。

下面从 E 构造出一个算法 F, 能以不可忽略的概率解决 GBDH 问题。F 的输入为群  $G_1, G_2,$  双线性映射  $e, G_1$  生成元  $P, G_1$  中的三个元素  $xP, yP, zP。$  其中:  $x, y, z \in Z_q^*, q$  是  $G_1, G_2$  的素数阶。F 可以访问 DBDH 预言机, 即输入  $\langle aP, bP, cP, W \rangle,$  如果  $W = e(P, P)^{abc},$  得到输出 1, 否则输出 0。F 的目标是计算出  $e(P, P)^{xyz}。$

F 选择随机数  $u, v \in \{1, \dots, \mu_1\}, p \in \{1, \dots, \mu_k\}。$  F 给 E 公共参数  $\langle G_1, G_2, e, p, xP \rangle,$  E 可以访问预言机  $H_1$  和  $H。$  F 要模拟游戏中所有的预言机, 并回答 E 的询问, 如下所示:

a)  $H_1(A)。$  F 通过维护列表 H1-List  $\langle A, r_A, Q_A \rangle$  来模拟  $H_1$  预言机。输入  $A \in \{0,1\}^*,$  如果 A 已经在 H1-List 中, F 输出  $Q_A;$  否则, 判断 A 是否为  $H_1$  询问的第  $v$  个 ID。如果是, 输出  $Q_A = yP,$  添加元组  $\langle A, \perp, Q_A \rangle$  到 H1-List, 初始化新用户 A; 如果不是, 选择随机数  $r_A \in Z_q^*,$  输出  $Q_A = r_A P,$  添加元组  $\langle A, r_A, Q_A \rangle$  到 H1-List, 初始化新用户 A, 私钥为  $\langle D_A = r_A xP, x_A \rangle,$  公钥为  $P_A = x_A P。$

假定 U 是  $H_1$  询问的第  $u$  个 ID, V 是第  $v$  个 ID。

F 维护一个会话密钥列表 G-List。对于 V 的每次会话, 在 G-List 中都有一项  $\langle B, n, sk_{V,B}^n \rangle,$  表示 V 与 B 的第 n 次会话, 会话密钥  $sk_{V,B}^n$  初始化为  $\perp。$

b) Send(A, B, m)。攻击者 E 代表 B 向 A 发送信息 m。如果  $A = U, B = V,$  并且是 U、V 的第 p 次密钥协商, 那么 F 从 H1-List 中提取  $r_U。$  其中:  $H_1(U) = r_U P,$  输出  $zH_1(U) = r_U zP, zP;$  否则, F 选择随机数  $\alpha \in Z_q^*,$  输出  $\alpha H_1(A), \alpha P。$

c)  $H(s)。$  F 通过维护列表 H-List  $\langle s, \iota \rangle$  来模拟 H 预言机。

其中:  $t \in \{0, 1\}^l$ 。

如果  $s$  已经在 H-List 中, F 输出  $t$ ; 否则, 如果  $s$  不是这种形式  $\langle k, p1, p2, V, B, PT \rangle$  或者  $\langle k, p1, p2, B, V, PT \rangle$  (其中:  $B$  是某个 ID,  $k \in G_2, p1, p2 \in G_1, PT \in G_1^A$ ), 那么 F 选择随机数  $t \in \{0, 1\}^l$ , 添加  $\langle s, t \rangle$  到 H-List, 输出  $t$ 。

如果  $s$  是这种形式  $\langle k, p1, p2, V, B, PT \rangle$  或者  $\langle k, p1, p2, B, V, PT \rangle$  (其中:  $B$  是某个 ID,  $k \in G_2, p1, p2 \in G_1, PT \in G_1^A$ )。对于 G-List 中  $sk_{V,B}^n \neq \perp$  的每一项, F 作如下操作。如果该项对应的会话  $(V, B, n)$  中,  $V$  收到  $W_B, T_B$ , 并发送  $W_V = \alpha Q_V, T_V = \alpha P$ , 那么 F 向 DBDH 预言机输入  $\langle yP, \alpha H_1(B) + W_B, xP, k \rangle$ , 预言机输出  $b$ 。如果某次 DBDH 预言机输出的  $b$  为 1, 那么 F 输出  $sk_{V,B}^n$ ; 否则 F 输出随机数  $t \in \{0, 1\}^l$ , 添加  $\langle s, t \rangle$  到 H-List。

d) Reveal  $(A, B, n)$ 。E 询问会话  $(A, B, n)$  的会话密钥。

如果  $(A, B, n) = (U, V, p)$ , 那么 F 终止。

如果  $(A, B, n) \neq (V, B, n)$ , F 输出  $sk_{A,B}^n$ ; 否则  $(A, B, n) = (V, B, n)$ , 假定在该会话中,  $V$  收到信息  $W_B, T_B$ , 并发送  $W_V = \alpha Q_V, T_V = \alpha P$ , F 作如下操作。

对 H-List 上的每一项  $\langle s, t \rangle$ , 如果  $s$  的格式符合  $\langle k, p1, p2, V, B, PT \rangle$  或者 (其中:  $B$  是某个 ID,  $k \in G_2, p1, p2 \in G_1, PT \in G_1^A$ )。F 向 DBDH 预言机输入  $\langle yP, \alpha H_1(B) + W_B, xP, k \rangle$ , 得到预言机的输出  $b$ 。如果有某次  $b$  为 1, 那么 F 令  $sk = t$ 。其中:  $t = H(s)$ 。否则, F 选择随机数  $sk \in \{0, 1\}^l$ , 然后, F 设置 G-List 上的值  $sk_{V,B}^n$  并输出  $sk$ 。

e) Long-Term key reveal  $(A)$ 。返回用户 A 的长期私钥。

f) Ephemeral key reveal  $(A, B, n)$ 。返回会话的一个临时私钥。

F 对透露长期私钥和临时私钥的请求进行综合考虑, 除了对于会话  $(U, V, p)$  和与它匹配的会话, 不能同时透露用户 U 的长期私钥和临时私钥, 或者 V 的长期私钥和临时私钥, 其他请求均给予回应。

g) Test  $(A, B, n)$ 。在某一时刻, E 发出 test 请求。如果 E 没有选中会话  $(U, V, p)$ , F 终止。F 随机选取  $b \in \{0, 1\}$ , 如果  $b = 1$ , F 输出 reveal  $(U, V, p)$  的结果; 否则, 输出随机数。

E 最终输出一个比特  $b'$ , 如果  $b' = b$ , 那么 E 赢得这个游戏。

接下来, 分析 F 如何通过赢得游戏的 E 来解决 GBDH 问题。

在 test query 中 E 选中会话  $(U, V, p)$  的概率是  $1/\mu_1^2 \mu_2$ 。E 赢得游戏的概率是  $\eta$ , 在 E 赢得游戏的情况下, 有压倒性的概率  $1 - 1/2^l$ , E 向 H 预言机发过询问  $SS_{U,V}^0$  ( $SS_{U,V}^0$  表示未经过 H 计算的会话信息串); 否则 E 是无法区分随机数和真实会话密钥的。F 从 H-List 中选取一项  $\langle s, t \rangle$ 。其中  $s$  符合  $\langle k, p1, p2, V, B, PT \rangle$  或者  $\langle k, p1, p2, B, V, PT \rangle$  (其中:  $B$  是某个 ID,  $k \in G_2, p1, p2 \in G_1, PT \in G_1^A$ ), 并猜想  $S = SS_{U,V}^0$ , 猜对的概率至少为  $1/\mu_2$ 。

F 从 H-List 中提取  $r_U (H_1(U) = r_U P)$ , 计算  $D_U = r_U xP$ 。而  $H_1(V) = yP, W_U = r_U zP$ , 因此, 如果  $S = SS_{U,V}^0$ , 那么  $k = e(D_U, W_V + zyP) = e(r_U xP, W_V) \cdot e(r_U xP, zyP)$ , 然后, F 输出  $(k/\delta)^{1/r_U}$  作为  $e(P, P)^{xyz}$  的猜想。其中  $\delta = e(r_U xP, W_V)$ 。此时, F 以不可忽略的概率  $\eta/\mu_1^2 \mu_2 (1 - 1/2^l)$  解决了 CBDH 问题。

F 在拥有 DBDH 预言机的情况下能以不可忽略的概率解决 CBDH 问题, 即 F 能以不可忽略的概率解决 GBDH 问题, 这与 GBDH 问题是困难的矛盾。因此, 证明了该协议在 ECK 模型下的安全性。

3.2 安全属性分析

1) 已知会话密钥安全 由于在产生会话密钥时使用了临时值  $(a, b)$ , 一个会话密钥被知道了不影响以前的或者将来的会话。协议的不同运行会产生不同的会话密钥, 即使是相同的通信参与者。

2) 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  $K_{AB}$  需要知道  $a$ , 而计算  $K_{BA}$  需要知道  $b$ 。即使是 KGC 也不能恢复出会话密钥。

3) 密钥妥协伪装安全 假设攻击者 E 知道 A 的私钥。如果 E 拦截  $W_B, T_B, P_B$  并把  $W'_B, T'_B, P'_B$  传递给 A, E 仍然无法得到会话密钥, 因为计算  $K_{AB}$  需知道  $a$ , 计算  $K_{BA}$  需要知道  $D_B$ 。

4) 未知密钥共享安全 如果 A 要和 B 协商会话密钥, A 使用 B 的公钥  $P_B$  和身份  $Q_B$  来计算会话密钥。因此, C 如果想算出同样的会话密钥, 必须得到对应的私钥  $S_B = \langle D_B, x_B \rangle$ , 而  $D_B$  只有 KGC 和实体 B 知道, 因此 C 无法计算出会话密钥。

5) 已知临时会话信息安全 假设攻击者得到会话的临时私钥  $a$  和  $b$ , 它仍然无法计算  $K = e(Q_A, Q_B)^{s(a+b)}$ 。但是如果攻击者是 KGC, 那么它就能计算出  $K$ 。此时, 会话密钥的安全性则由  $x_A x_B P$  来保证, 因为 KGC 不知道  $x_A$  和  $x_B$  的值。

3.3 效率分析与比较

Al-Riyami 等人<sup>[1]</sup>提出的无证书密钥协商协议, 计算量比较大, 协议的每一方需计算四个配对。Mandt<sup>[3]</sup>对它进行了改进, 协议的每一方只需计算两个配对, 但是存在 KCI 攻击。

在新方案中, 参与密钥协商的每一方需要计算一个配对, 三个椭圆曲线点乘, 一个椭圆曲线点的加法。这几种运算中, 配对的计算量比较大, 因此相对于之前提出的密钥协议, 本文提出的方案效率较高。不同协议的效率比较如表 1 所示。

表 1 不同协议的效率比较

| 协议                      | 配对 | 点乘 | 加法 | 幂 |
|-------------------------|----|----|----|---|
| AP' s <sup>[1]</sup>    | 4  | 2  | 0  | 1 |
| Mandt' s <sup>[3]</sup> | 2  | 3  | 1  | 1 |
| 新方案                     | 1  | 5  | 1  | 0 |

4 结束语

本文提出了一种在无证书公钥密码体系下的密钥协商方案, 该方案是第一个被证明 ECK 模型安全的无证书密钥协商方案, 能满足期望的安全属性。与其他无证书密钥协议分析比较, 具有较好的安全性和效率。

参考文献:

[1] AL-RIYAMI S S, PATERSON K. Certificateless public key cryptography[C]// Proc of ASIACRYPT 2003. Berlin: Springer-Verlag, 2003:452-473.

[2] LAMACCHIA B, LAUTER K, MITYAGIN A. Stronger security of authenticated key exchange[C]// Proc of Sec 2007. Berlin: Springer-Verlag, 2007:1-16.

[3] MANDT T K. Certificateless authenticated two-party key agreement protocols[D]. Oppland: Gjøvik University College, 2006.

[4] BLAKE-WILSON S, JOHNSON 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.

[5] KUDLA C J. Special signature schemes and key agreement protocols [D]. London: University of London, 2006.