第41卷 第6A期
2014年6月

计 算 机 科 学
Computer Science

Vol. 41 No. 6A
June 2014

航空移动自组网中簇间节点密钥协商方案

孙 凌[1] 田 源[1] 黄后彪[2]

(河南牧业经济学院 郑州 450044)[1] (解放军信息工程大学 郑州 450004)[2]

摘 要 针对航空移动自组网高动态和资源受限的特点,提出了一种适用于簇间节点的无证书密钥协商方案,在随机预言机模型下证明了该方案身份认证过程中的签名是存在性不可伪造的,并分析证明了只要每个节点都还存有一个秘密值,那么协商的会话密钥就是安全的。本方案没有使用复杂的双线性对运算、指数运算和求逆运算,经过与其它现有的无证书密钥协商方案比较,本方案的计算复杂度是最低的。

关键词 航空移动自组网,无证书密钥协商,随机预言机模型,无双线性对

中图法分类号 TP309.2 **文献标识码** A

Nodes Key Agreement Scheme between Clusters in Aeronautical Mobile Ad hoc Network

SUN Ling[1] TIAN Yuan[1] HUANG Hou-biao[2]

(Henan University of Animal Husbandry & Economy, Zhengzhou 450044, China)[1]

(The PLA Information Engineering University, Zhengzhou 450004, China)[2]

Abstract According to the characteristics of the resource constraints and high dynamic of the aeronautical mobile ad hoc network, we proposed a certificateless key agreement scheme applicable to nodes between clusters. The signature scheme was proved to be secure in the random oracle model and the session key was proved to be secure as long as each node still has at least one security secret value. Our scheme avoids pairing computation, exponentiation computation and inverse computation. The computational cost is the lowest in our scheme compared with all the other existing certificateless key agreement schemes.

Keywords Aeronautical mobile ad hoc Network, Certificateless key agreement, Random oracle model, Pairing-free

1 引言

近年来,随着对移动自组网应用的研究,一些研究协会和研究者开始把它们应用在航空通信中,创造了一个新的研究领域——航空移动自组网。航空移动自组网的基本思想[1]是:一定范围内的飞机节点之间可以互相转发控制指令信息,交换各自的飞行状态、感知信息等数据,并自动地连接,建立起一个 MANET(mobile ad hoc network)。在该网络中,每个飞行器不仅是一个收发器,而且还是一个路由器,可采用多跳的方式把数据转发给更远的飞行器。图1所示为航空移动自组网模型。航空移动自组网模型分为两层:上层为骨干网络,网络中节点飞行高度高于下层网络中的飞机节点。下层为一般节点网络。飞机节点通过分簇算法,选取飞行方向、速度以及间距都相适应的节点形成一个簇。簇内节点进行组播通信,而簇间节点进行单播通信。由于航空环境的高动态性对于簇间节点的通信安全形成了巨大的挑战,因此需要一个安全、高效的密钥协商协议使飞机节点之间通过不安全信道产生一个共享会话密钥,来为后续的会话通信提供认证、保密或完整性等安全服务。

2003年,Al-Riyami 和 Paterson[2] 在亚密会上首次提出了无证书公钥密码体制的概念,它解决了基于身份密码体制中用户密钥托管的问题和证书存储、管理问题。在此之后,许多研究者都相继提出了不同的无证书两方认证密钥协商协议[3,4],然而这些方案都无法抵抗密钥泄露扮演攻击和临时私钥泄露攻击[5]。而安全的方案,效率又不高,如 Lippold[6] 提出了一种安全的无证书两方认证密钥协商协议,但是该方案中使用了十次双线性对运算和五次指数运算,计算效率太低。根据文献[7]运行一个512位双线性对运算需要花费20ms,进行一个1024位素数指数操作需要8.8ms,而运行一次双线性对操作的时间至少是椭圆曲线上点乘运算的21倍[8]。Liu[9] 也提出了一种安全的无证书两方认证密钥协商协议,虽然没有使用到双线性对运算和指数运算,但是该方案中的一次求逆运算相当于80次的点乘运算[10],计算复杂度也较高。因此现有两方密钥协商方案对于资源、能量受限、高动态的航空移动自组网都不适用。本文提出了一种航空移动自组网环境下簇间节点的会话密钥协商方案,本方案在安全方面优点如下:(1)无密钥托管;(2)抗密钥泄露扮演攻击;(3)抗临时私钥泄露攻击。除非攻击者能够解决基于椭圆曲线上的 Diffie-Hellman 问题和离散对数问题,否则只要参与密钥协商的每个节点至少有一个秘密值未泄露,那么本方案就是安全的。在计算复杂度方面,本方案没有使用到双线性对运

本文受河南省高等学校青年骨干教师资助基金2011资助。

孙 凌(1976—),硕士,副教授,主要研究方向为网络安全、数据库;田 源(1981—),硕士,讲师,主要研究方向为多媒体技术;黄后彪(1983—),硕士,主要研究方向为网络安全。

算、指数运算和求逆运算，只涉及到了椭圆曲线上的点乘运算，而一次点乘运算的时间大约为 1ms，在效率方面优于其他无证书两方认证密钥协商方案。因此，本方案适用于航空移动自组网的特殊环境。

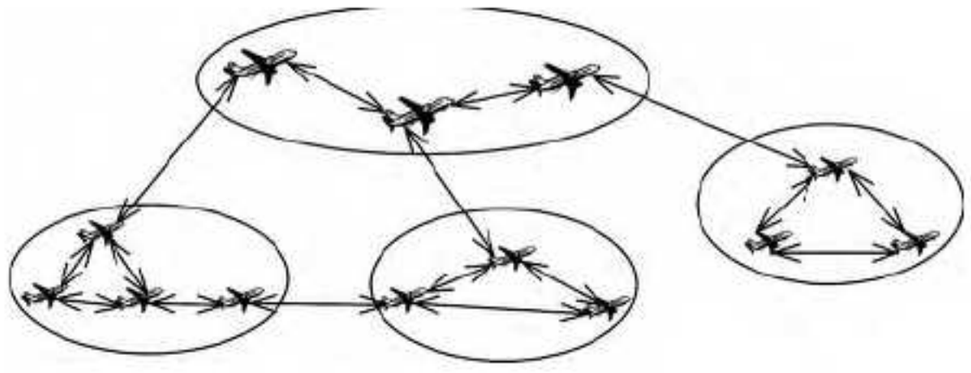

图 1　航空移动自组网模型

2　有关困难问题

椭圆曲线上 Diffie-Hellman 问题：对于椭圆曲线 $E(F_p)$，G 是 $E(F_p)$ 上的循环加法群，G 的生成元为 P，$a,b\in Z_q^*$，令 $A=aP,B=bP$。在已知 A,B 的条件下，求 $C=abP$ 的问题，称为椭圆曲线上 Diffie-Hellman 问题。

椭圆曲线上的离散对数问题：对于椭圆曲线 $E(F_p)$，G 是 $E(F_p)$ 上的循环加法群，G 的生成元为 P，$A\in G$。在已知 A，P 的条件下，求解整数 a，使得 $aP=A$ 的问题，称为椭圆曲线上的离散对数问题。

3　密钥协商方案

(1) 系统建立：PKG 选择椭圆曲线 $E(F_p)$ 上的 q 阶循环加法群 G，G 的生成元为 P。随机选择 $s\in Z_q^*$ 作为系统主密钥，系统公钥为 $P_{pub}=sP\in G$。定义以下安全哈希函数：$H_1:\{0,1\}^*\times G\to Z_q^*$，$H_2:\{0,1\}^*\to Z_q^*$，$H_3:\{0,1\}^*\times\{0,1\}^*\times G^7\to\{0,1\}^k$。PKG 妥善保管 s，公开系统参数 $\{G,q,P,P_{pub},H_1,H_2,H_3\}$。

(2) 私钥产生：节点 i 的身份标识为 ID_i，i 随机选择 $s_i\in Z_q^*$ 作为长期私钥，计算公钥 $S_i=s_iP$。PKG 按如下步骤计算节点 i 的部分私钥：

① 随机选择 $r_i\in Z_q^*$，计算 $R_{i1}=r_iP,R_i=R_{i1}+S_i$；

② 令 $h=H_1(ID_i,R_i)$，计算部分私钥 $d_i=r_i+sh$。

PKG 将 d_i 和 R_i 通过安全信道发送给节点 i。i 通过检验 $(d_i+s_i)P=R_i+H_1(ID_i,R_i)P_{pub}$ 是否成立来验证部分私钥的正确性。

(3) 签名：节点 A 随机选择 $y_A\in Z_q^*$ 作为临时私钥，计算临时公钥 $Y_A=y_AP$。节点 A 对消息 $m\in\{0,1\}^*$ 进行签名：计算 $e=H_2(ID_A,m,R_A,Y_A),h=H_1(ID_A,R_A),z=hy_A+e(d_A+s_A)$，则节点 A 对消息 m 的签名为 $\sigma=(R_A,Y_A,z)$。A 发送消息 $\langle\sigma,m,ID_A\rangle$ 给节点 B。

(4) 验证：节点 B 收到 A 发送的消息后：

① 计算 $h=H_1(ID_A,R_A)$ 和 $e=H_2(ID_A,m,R_A,Y_A)$；

② 验证等式

$$zP=hY_A+e(R_A+S_A+hP_{pub}) \tag{1}$$

是否成立。若成立则输出“真”，节点 B 通过对节点 A 的身份认证。

(5) 密钥协商：节点 B 随机选择 $y_B\in Z_q^*$，计算 $Y_B=y_BP$，$D_A=R_A+hP_{pub}$，发送消息 $\langle Y_B,ID_B,R_B\rangle$ 给节点 A，并计算：

$$K_{B1}=s_B(S_A+D_A+Y_A)=s_B(s_AP+d_AP+y_AP)$$

$$K_{B2}=d_B(S_A+D_A+Y_A)=d_B(s_AP+d_AP+y_AP)$$

$$K_{B3}=y_B(S_A+D_A+Y_A)=y_B(s_AP+d_AP+y_AP)$$

节点 A 收到 B 发送的消息后，计算 $h'=H_1(ID_B,R_B),D_B=R_B+h'P_{pub}$，计算：

$$K_{A1}=S_B(s_A+d_A+y_A)=s_B(s_AP+d_AP+y_AP)$$

$$K_{A2}=D_B(s_A+d_A+y_A)=d_B(s_AP+d_AP+y_AP)$$

$$K_{A3}=Y_B(s_A+d_A+y_A)=y_B(s_AP+d_AP+y_AP)$$

由以上计算可知：

$$K_{A1}=K_{B1}=K_1$$

$$K_{A2}=K_{B2}=K_2$$

$$K_{A3}=K_{B3}=K_3$$

节点 A 和节点 B 可各自算出它们的会话密钥 $K=H_3(K_1,K_2,K_3)$。

4　安全性证明

4.1　签名不可伪造性

本节将针对两种类型的攻击者，利用随机预言机模型来证明本方案的签名是不可伪造的。

随机预言机模型证明过程为：首先将整个证明过程定义为一个仿真游戏，在模型中有随机预言机、仿真者和攻击者。仿真者对攻击者所有的查询进行回答，在仿真游戏的最后，仿真者给出事先确定的挑战，如果攻击者完成该挑战，则仿真游戏成功。但是由于开始确定的挑战中包含仿真者用来解答方案所基于的困难问题的知识，如果仿真游戏成功的概率为不可忽略的值，则困难问题在该环境下不再是困难的。这与现实环境中已知困难问题的不可计算性相矛盾，因此该攻击者实际是不存在的，方案在模型下是安全的。

对于本文的签名方案，存在以下两种类型的攻击者：

类型 1　攻击者不知道节点的长期私钥和部分私钥。

类型 2　攻击者知道节点的系统主密钥或部分私钥，但是不知道节点的长期私钥。

定理 1　本方案对于类型 1 的攻击者是存在性不可伪造的。

证明：B 是一个 ECDLP 问题的解决者，调用 A 作为子程序，在一个概率多项式时间（probabilistic polynomial time，PPT）内解决 ECDLP 问题。设 (P,aP) 是群 G 上的一个任意公私钥对，B 作为 A 的挑战者进行以下游戏：

B 运行 Step 算法，定义系统公钥 $P_{pub}=aP$，P 是椭圆曲线上阶为 q（$q>2^k$，k 是安全参数）的一个点，生成系统参数 $params:\{q,G,P,P_{pub},H_1,H_2\}$，$B$ 随机选取 $ID_I(1\leqslant I\leqslant q_{H_1}$，$q_{H_1}$ 是 A 进行 H_1 查询的最大次数）作为此次游戏挑战者的身份。随机选取 $h_I\in Z_q^*$，令 $R_I=aP-h_IaP$，定义 $h_I=H_1(ID_I,R_I)$，将 (ID_I,R_I,h_I) 存入列表 L_1 中。B 将系统参数发送给攻击者 A。A 进行如下查询：

H_1 查询：A 输入 (ID_i,R_i)，B 查询列表 L_1。如果列表 L_1 中存有对应的记录 (ID_i,R_i,h_i)，就将 h_i 返回给 A。如果没有，则 B 随机选择 $h_i\in Z_q^*$，将 (ID_i,R_i,h_i) 加入到列表 L_1 中，并将 h_i 返回给 A。

H_2 查询：A 以 (m_i,ID_i,Y_i,R_i) 作为输入，B 查询列表 L_2。如果列表 L_2 中存有对应的记录，就返回已有值给 A。如果没有，则 B 随机选择 $e_i\in Z_q^*$，将 (m_i,ID_i,Y_i,R_i,e_i) 加入到列表 L_2 中，并返回 e_i 给 A。

部分私钥查询：B 维护一个列表 L_E。A 以 ID_i 作为输入：

(1)如果 $ID_i=ID_I$，则 B 终止模拟，并输出“失败”；

(2)如果 $ID_i\neq ID_I$，则 B 随机选取 $s_i\in Z_q^*$ 作为 ID_i 的长期私钥，然后随机选取 $d_i,h_i\in Z_q^*$，令 $h_i=H_1(ID_i,R_i)$（若 $H_1(ID_i,R_i)$ 已经存在，则 B 终止模拟，但是这种情况发生的概率最大为 $(q_{H_1}+q_E)/2^{k+1}$，其中 q_E 表示查询部分私钥解析预言机的最多次数），计算 $R_i=d_iP+s_iP-h_iaP$。将 (ID_i,R_i,h_i) 加入到列表 L_1 中，(ID_i,R_i,d_i,s_i) 加入到列表 L_E 中，并将 (d_i,R_i) 返回给 A。

长期私钥查询：若 $ID_i=ID_I$，则 B 终止模拟，并输出“失败”。否则返回 s_i 给 A。

签名查询：A 以 (m_i,ID_i) 作为输入：

(1)如果 $ID_i=ID_I$，则 B 随机选取 $z_I,e_I\in Z_q^*$，令 $R_I=aP-h_IaP$，定义 $e_I=H_2(ID_I,m_i,R_I,Y_I)$（若 $H_2(ID_I,m_i,R_I,Y_I)$ 已经被定义，则 B 终止模拟，但是出现这种情况的概率最大为 $(q_{H_2}+q_S)/2^k$，其中 q_S 是查询签名解析预言机的最多次数），计算 $h_IY_I=z_IP-e_I(R_I+h_IP_{pub})$，并将 (R_I,Y_I,z_I) 返回给 A。

(2)若 $ID_i\neq ID_I$，由于 B 拥有 ID_i 的部分私钥和长期私钥，因此签名是平凡的。

伪造签名：A 对消息 m' 关于身份 ID' 的签名为 (R'_I,Y'_I,z')，ID' 并没有提交过给部分私钥预言机和长期私钥预言机进行查询，而 (m',ID') 也未进行过签名查询。若 $ID'\neq ID_I$ 且 $R'\neq R_I$，则 B 终止模拟（B 不会终止模拟的概率 $\geqslant 1/q_{H_1}$）。否则根据分叉引理规约方法[11]可知，在概率多项式时间内，存在算法 U 可以生成两个有效签名 $(m',ID_I,R_I,Y_I,e_1,z_1)$ 和 $(m',ID_I,R_I,Y_I,e_2,z_2)$ 且 $e_1\neq e_2$。因为在最开始就定义了 $h_I=H_1(ID_I,R_I)$，所以这里 h_I 不变。因此有以下等式成立：

$$h_IY_I=z_1P-e_1(R_I+h_IP_{pub}) \tag{2}$$

$$h_IY_I=z_2P-e_2(R_I+h_IP_{pub}) \tag{3}$$

由式(2)、式(3)可得：

$$(z_1-z_2)P=(e_1-e_2)ap \tag{4}$$

由式(4)可得：

$$a=\frac{(z_1-z_2)}{(e_1-e_2)}$$

所以 B 解决了椭圆曲线上的离散对数困难问题。

定理 2　本方案对于类型 2 的攻击者是存在性不可伪造的。

证明：B 是一个 ECDLP 问题的解决者，调用 A 作为子程序，在一个概率多项式时间（probabilistic polynomial time，PPT）内解决 ECDLP 问题。设 (P,aP) 是群 G 上的一个任意公私钥对，B 作为 A 的挑战者进行以下游戏。

B 运行 Step 算法，随机选取 $s\in Z_q^*$ 作为系统私钥，定义系统公钥 $P_{pub}=sP$，P 是椭圆曲线上阶为 q（$q>2^k$，k 是安全参数）的一个点，生成系统参数 $params:\{q,G,P,P_{pub},H_1,H_2\}$，$B$ 随机选取 $ID_I(1\leqslant I\leqslant q_{H_1},q_{H_1}$ 是 A 进行 H_1 查询的最大次数）作为此次游戏挑战者的身份。B 将系统参数发送给攻击者 A。A 进行如下查询：

H_1 查询：A 输入 (ID_i,R_i)，B 查询列表 L_1。如果列表 L_1 中存有对应的记录 (ID_i,R_i,h_i)，就将 h_i 返回给 A。如果没有，则 B 随机选择 $h_i\in Z_q^*$，将 (ID_i,R_i,h_i) 加入到列表 L_1 中，并将 h_i 返回给 A。

H_2 查询：A 以 (m_i,ID_i,Y_i,R_i) 作为输入，B 查询列表 L_2。如果列表 L_2 中存有对应的记录，就返回已有值给 A。如果没有，则 B 随机选择 $e_i\in Z_q^*$，将 (m_i,ID_i,Y_i,R_i,e_i) 加入到列表 L_2 中，并返回 e_i 给 A。

部分私钥查询：B 维护一个列表 L_E。A 以 ID_i 作为输入：

(1)如果 $ID_i=ID_I$，则 B 令 $R_i=aP$，查询列表 L_1，找到表中相对应的记录 (ID_i,R_i,h_i)。然后随机选取 $r_i\in Z_q^*$，求得 $d_i=r_i+sh_i$。将 $(ID_i,R_i,d_i,\perp)$ 加入到列表 L_E 中（其中 $\perp$ 表示未知的长期私钥），将 R_i,d_i 返回给 A。

(2)若 $ID_i\neq ID_I$，则 B 随机选取 $r_i',s_i\in Z_q^*$，求得 $R_i=(r_i'+s_i)P$，$d_i=r_i'+sh_i$，将 (ID_i,R_i,d_i,s_i) 加入到列表 L_E 中，将 R_i,d_i 返回给 A。

长期私钥查询：如果 $ID_i=ID_I$，则 B 终止模拟，并输出“失败”。否则 B 返回 s_i 给 A。

签名查询：A 以 (m_i,ID_i) 作为输入：

(1)如果 $ID_i=ID_I$，则 B 随机选取 $z_I,e_I\in Z_q^*$，令 $R_i=aP$，从列表 L_1 中调出对应的记录 (ID_i,R_i,h_i)，定义 $e_i=H_2(ID_i,m_i,R_i,Y_i)$（若 $H_2(ID_I,m_i,R_I,Y_I)$ 已经被定义，则 B 终止模拟，但是出现这种情况的概率最大为 $(q_{H_2}+q_S)/2^k$，其中 q_S 是查询签名解析预言机的最多次数），计算 $h_iY_i=z_iP-e_i(R_i+h_iP_{pub})$，并将 (R_i,Y_i,z_i) 返回给 A。

(2)若 $ID_i\neq ID_I$，由于 B 拥有 ID_i 的部分私钥和长期私钥，因此签名是平凡的。

伪造签名：A 对消息 m' 关于身份 ID' 的签名为 (R_I',Y_I',z')，ID' 并没有提交过给长期私钥预言机进行查询，而 (m',ID') 也未进行过签名查询。若 $ID'\neq ID_I$ 且 $R'\neq R_I$，则 B 终止模拟（B 不会终止模拟的概率 $\geqslant 1/q_{H_1}$）。否则根据分叉引理规约方法[11]可知，在概率多项式时间内，存在算法 U 可以生成两个有效签名 $(m',ID_I,R_I,Y_I,e_1,z_1)$ 和 $(m',ID_I,R_I,Y_I,e_2,z_2)$ 且 $e_1\neq e_2$。因此有以下等式成立：

$$h_IY_I=z_1P-e_1(R_I+h_IP_{pub}) \tag{5}$$

$$h_IY_I=z_2P-e_2(R_I+h_IP_{pub}) \tag{6}$$

由式(5)、式(6)可得：

$$(z_1-z_2)P=(e_1-e_2)(a+h_Is)P \tag{7}$$

由式(7)可得：

$$a=\frac{(z_1-z_2)}{(e_1-e_2)}-h_Is$$

所以 B 解决了椭圆曲线上的离散对数困难问题。

若攻击者攻破了本方案，则说明在部分私钥查询、签名查询和伪造签名时 B 均不会停止模拟，此概率大于 $((q_{H_1}+q_E)/2^{k+1})((q_{H_2}+q_S)/2^k)(1/q_{H1})$。

4.2　密钥安全性

本文的方案是基于椭圆曲线上 Diffie-Hellman 问题和椭圆曲线上的离散对数问题提出的，只要参与会话密钥协商的节点中，每方至少有一个没有泄露的秘密值，则本方案就是安全的。

本方案满足以下几种安全属性：

(1)已知密钥安全：攻击者已知节点之间协商的本次会话密钥，但无法根据已获得的会话密钥算出本次会话之前和以后的会话密钥。

(2)认证性:如果节点 A 不知道节点 B 的身份,节点 A 不会与节点 B 协商会话密钥。

(3)抗密钥泄露扮演攻击:当节点 A 与节点 B 进行会话密钥协商时,如果节点 A 的长期私钥被攻击者获得,此时攻击者只能向节点 B 假冒节点 A,反之则不行。

(4)长期私钥泄露安全:如果参与会话密钥协商的节点 A 与节点 B 的长期私钥被攻击者获得,攻击者无法根据此长期私钥计算出本次会话之前的会话密钥。

(5)PKG 前向安全:如果 PKG 的主私钥被攻击者获得,攻击者无法算出本次会话密钥协商之前的会话密钥。

(6)无密钥控制:任何攻击者和会话密钥协商的参与者,都不能将会话密钥控制成其预先选定的值。

(7)临时私钥泄露安全:即使参与协商的节点临时私钥被泄露,也不会影响本次会话密钥协商的安全。

(8)无密钥托管:即使参与协商的节点部分私钥被泄露,也不会影响本次会话密钥协商的安全。

我们在最强攻击者的攻击模型下(参与会话密钥协商的节点,每方只保存一个秘密值,允许攻击者获取其他 4 个秘密值),分 9 种情况来讨论本方案的安全性:

(1)攻击者已知 d_A, d_B, s_A, s_B,但是 y_A, y_B 是安全的,未泄露。攻击者要想计算出最后的会话密钥 K,必须先得到 $y_A y_B P$,再算出 K_3。而在已知 $y_A P, y_B P$ 的情况下,要得出 $y_A y_B P$,面临着解决椭圆曲线上 Diffie-Hellman 问题(ECDH)。在已知 $y_A P, y_B P$ 的情况下,要得出 y_A, y_B,面临着解决椭圆曲线上的离散对数问题(ECDLP)。此时,本方案满足 PKG 前向安全,长期私钥泄露安全和无密钥托管。

(2)攻击者已知 d_A, d_B, y_A, y_B,但是 s_A, s_B 是安全的,未泄露。攻击者要想计算出最后的会话密钥 K,必须先得到 $s_A s_B P$,再算出 K_1。而在已知 $s_A P, s_B P$ 的情况下,要得出 $s_A s_B P$,面临着解决 ECDH 问题。在已知 $s_A P, s_B P$ 的情况下,要得出 s_A, s_B,面临着解决 ECDLP 问题。此时,本方案满足 PKG 前向安全,临时私钥泄露安全和无密钥托管。

(3)攻击者已知 d_A, d_B, y_A, s_B,但是 s_A, y_B 是安全的,未泄露。攻击者要想计算出最后的会话密钥 K,必须先得到 $s_A y_B P$,再算出 K_3。而在已知 $s_A P, y_B P$ 的情况下,要得出 $s_A y_B P$,面临着解决 ECDH 问题。在已知 $s_A P, y_B P$ 的情况下,要得出 s_A, y_B,面临着解决 ECDLP 问题。此时,本方案满足 PKG 前向安全和无密钥托管。

(4)攻击者已知 d_A, d_B, s_A, y_B,但是 y_A, s_B 是安全的,未泄露。攻击者要想计算出最后的会话密钥 K,必须先得到 $y_A s_B P$,再算出 K_1。而在已知 $y_A P, s_B P$ 的情况下,要得出 $y_A s_B P$,面临着解决 ECDH 问题。在已知 $y_A P, s_B P$ 的情况下,要得出 y_A, s_B,面临着解决 ECDLP 问题。此时,本方案满足 PKG 前向安全和无密钥托管。

(5)攻击者已知 s_A, s_B, y_A, y_B,但是 d_A, d_B 是安全的,未泄露。攻击者要想计算出最后的会话密钥 K,必须先得到 $d_A d_B P$,再算出 K_2。而在已知 $d_A P, d_B P$ 的情况下,要得出 $d_A d_B P$,面临着解决 ECDH 问题。在已知 $d_A P, d_B P$ 的情况下,要得出 d_A, d_B,面临着解决 ECDLP 问题。此时,本方案满足长期私钥泄露安全和临时私钥泄露安全。

(6)攻击者已知 s_A, s_B, y_A, d_B,但是 d_A, y_B 是安全的,未泄露。攻击者要想计算出最后的会话密钥 K,必须先得到 $d_A y_B P$,再算出 K_3。而在已知 $d_A P, y_B P$ 的情况下,要得出 $d_A y_B P$,面临着解决 ECDH 问题。在已知 $d_A P, y_B P$ 的情况下,要得出 d_A, y_B,面临着解决 ECDLP 问题。此时,本方案满足长期私钥泄露安全和无密钥托管。

(7)攻击者已知 s_A, s_B, d_A, y_B,但是 y_A, d_B 是安全的,未泄露。攻击者要想计算出最后的会话密钥 K,必须先得到 $y_A d_B P$,再算出 K_2。而在已知 $y_A P, d_B P$ 的情况下,要得出 $y_A d_B P$,面临着解决 ECDH 问题。在已知 $y_A P, d_B P$ 的情况下,要得出 y_A, d_B,面临着解决 ECDLP 问题。此时,本方案满足长期私钥泄露安全和无密钥托管

(8)攻击者已知 y_A, y_B, s_A, d_B,但是 d_A, s_B 是安全的,未泄露。攻击者要想计算出最后的会话密钥 K,必须先得到 $d_A s_B P$,再算出 K_1。而在已知 $d_A P, s_B P$ 的情况下,要得出 $d_A s_B P$,面临着解决 ECDH 问题。在已知 $d_A P, s_B P$ 的情况下,要得出 d_A, s_B,面临着解决 ECDLP 问题。此时,本方案满足临时私钥泄露安全,PKG 前向安全和无密钥托管。

(9)攻击者已知 y_A, y_B, d_A, s_B,但是 s_A, d_B 是安全的,未泄露。攻击者要想计算出最后的会话密钥 K,必须先得到 $s_A d_B P$,再算出 K_2。而在已知 $s_A P, d_B P$ 的情况下,要得出 $s_A d_B P$,面临着解决 ECDH 问题。在已知 $s_A P, d_B P$ 的情况下,要得出 s_A, d_B,面临着解决 ECDLP 问题。此时,本方案满足临时私钥泄露安全,PKG 前向安全和无密钥托管。

5 方案性能比较

本文提出的方案中没有使用复杂、耗时的双线性对运算、指数运算和逆运算,在密钥协商过程中只需要进行 7 次椭圆曲线上的点乘运算,计算复杂度很低。而且本方案只需要一轮通信,传输带宽占用得也非常少。本方案与文献[3,4]相比,无论在安全性还是在效率上都优于它们。与文献[5,8]相比,在相同安全性的前提下大大减少了计算开销,具有明显的效率优势。表 1 给出了本文提出的方案与同类方案的性能比较。

表 1 通信开销和安全性比较

性能 / 方案	双线性对运算	指数运算	逆运算	点乘运算	抗临时私钥泄露攻击	抗密钥泄露扮演攻击	密钥前向安全	PKG 前向安全
文献[3]方案	2	1	0	1	否	否	否	否
文献[4]方案	6	0	0	9	否	否	否	否
文献[6]方案	10	5	0	5	是	是	是	是
文献[9]方案	0	0	1	5	是	是	是	是
本文方案	0	0	0	7	是	是	是	是

运行一个 512 位双线性对运算需要花费 20ms,进行一个 1024 位素数指数操作需要 8.8ms[7]。运行一次双线性对操作的时间至少是椭圆曲线上点乘运算时间的 21 倍[8]。一次求逆运算相当于 80 次的点乘运算[10]。

结束语 在资源和带宽受限的高动态航空移动自组网环境下,簇间飞机节点的密钥协商协议具有特殊的要求。本文基于航空移动自组网的环境,提出了一种无证书两方密钥协商方案,该方案的安全性基于椭圆曲线上的 Diffie-Hellman 问题和椭圆曲线上的离散对数问题,在效率方面未采用双线性对、指数运算、逆运算这些复杂的运算,满足航空移动自组网环境高安全性和低计算复杂度的要求。

参 考 文 献

[1] 郑博,张衡阳,等. 航空自组网贪婪地理路由协议研究[J]. 传感器与微系统,2012,31(5):23-25

[2] Al-Riyami S S,Paterson K. Certificateless public key cryptography [C] // Asiacrypt' 2003 (LNCS 2894). Springer-Verlag, 2003:452-473

[3] Wu C H,Chen Z X. A new efficient certificateless signcryption scheme[C]//Preceedings of the ISISE2008. 2008:661-664

[4] Yuan Y M, Li D, Tian L W, et al. Certificateless signature scheme without random oracles[C]//Park J H,et al. eds. Proc. of the ISA2009 (LNCS5576). Heidelberg: Springer-Verlag, 2009:31-40

[5] 张福泰,孙银霞,等. 无证书公钥密码体制研究[J]. 软件学报, 2011,22(6):1317-1332

[6] Lippold G, Boyd C, Gonzalez NJM. Strongly secure certificateless key agreement[C]//Shacham H, Waters B, eds. Proc. of the Pairing-Based Cryptography-Pairing 2009. LNCS5671, Heidelberg: Springer-Verlag, 2009:206-230

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

[9] 刘文浩,许春香. 无证书两方密钥协商方案[J]. 软件学报,2011, 22(11):2843-2852

[10] 候爱琴,高宝建,等. 基于椭圆曲线的一种高效率数字签名[J]. 计算机应用与软件,2009,26(2):58-71

[11] Andrew C, Zhao Y L. Digital signatures from challenge-divided sigma-protocols[OL]. Proc. of the IACR Cryptology ePrint Archive, 2012

(上接第 362 页)

可,在这个关系式中,除了 a_{11} 外,我们还有 $\partial-1$ 种选择。对于整个矩阵来说,就是对矩阵 D 进行行变换后的结果。经过行变换后的矩阵,破解者很难确定矩阵中每一行上哪一项不为零,这样就从根本上消除了原始方案中的线性关系。

考虑到安全性,这两种措施应该同时采取,这样的改进工作不会对解密效率带来任何的影响,因为我们的工作主要是围绕者扩展变量展开的,而这些工作对合法的解密者来说却是透明的。每一次加密都要对矩阵 D 进行行变换,对扩展变量进行顺序调整。

总的来说,改进的关键之处就在于利用全排列的方法对对角矩阵和扩展变量进行了扰动,改变了变量的排列顺序,使破解者无法利用变量之间的顺序关系破解原有密码体制。

5 目的矩阵 D 的生成算法

我们需要对矩阵 D 的行变换设计专门的算法才能保证加密的要求。如果对矩阵 D 进行行变换应该有 ∂ !种,但如果 ∂ 较大,那么用来存储行变换结构的空间对整个加密过程来说会变得难以承受,所以我们在这里设计了一种类似的计算 ∂ !的算法。该算法并没有存储全部的行变换的结果,只是返回给调用程序一种行变换的结果。结果如下:

1. 初始化数组 $a[\partial]=\{1,2,\cdots,\partial\}$。

2. 生成 $[0,\partial-i)$ 之间的一个随机数 $subcript$,其中 $0\leqslant i<\partial$。

3. 将数组中下标为 $subcript$ 的元素输出,原数组将该元素删除

4. 将 i 加 1,然后返回步骤 2,直至原数组中元素为空。输出的元素序列即是 ∂ 个元素全排列的一种,即矩阵 D 行变换的一种。

此方法同样适用于对扩展变量的顺序调整,这里不再一一赘述。

结束语 聂旭云等人分析了多变量公钥密码扩展方案,并且发现了方案中的安全漏洞,但并未对其进行改进,我们从他们的破解方法中找到了改进方案的方法,并且给出了相关的证明。多变量公钥密码是抗量子攻击的一个重要组成部分,一旦量子计算机出现,该加密体制一定会有更广泛的应用前景和更高的学术价值。未来的工作是多变量公钥密码体制在云环境下[12]的应用范围。

参 考 文 献

[1] Ding Jin-tai, Schmidt D. Multivariable public-key cryptosystems [J]. Advances in Information Security, 2006, 3494(10): 288-304

[2] Ding Jin-tai. A new Variant of Matsumoto-Imai Cryptosystem through Perturbation[J]. Public Key Cryptography-PKC, 2004, 2947(12): 305-318

[3] Ding Jin-tai, Schmidt D. Rainbow a new Multivariable Polynomial Signature[J]. Applied Cryptography and Network Security, 2005, 3531(14): 164-175

[4] Ding Jin-tai, Schmidt D. Cryptanalysis of HFEv and Internal Perturbation of HFE[J]. Public key Cryptography-PKC, 2005, 3386(5): 288-301

[5] Faugere J C. A new efficient algorithm for computing Grobner bases(F4)[J]. Journal of Pure and Applied Algebra, 2009 (139): 61-88

[6] Yang Bo-yin. Public-Key Cryptography from New Multivariate Quadratic Assumptions[J]. Informa tion Security, 2010(5): 193-241

[7] Ding Jin-tai, Hu Lei, Nie Xun-yun, et al. High Order Linearization Equition (HOLLE) Attack on Multivariable Public Key [J]. Advances in Information Security, 2010(9): 126-134

[8] Fouque P A, Granboulan L, Stern J. Differential Cryptanalysis for Multivariate Scheme[J]. Advance In Cryptology EUROCRYPT, 2005, 3494(9): 341-353

[9] 王后珍,张焕国,王张宜,等. 一类具有安全加密功能的扩展 MQ 公钥加密体制[J]. 中国科学,2011,41(11):1297-1309

[10] Yang Bo-yin, Chen Jiun-ming. Building Secure Tame-like Multivariate Public-Key Cryptosystems The New TTS[J]. Information Security and Privacy, 2005, 354(7): 518-531

[11] 聂旭云,徐赵虎,廖永建,等. 多变量公钥密码扩展方案的安全性分析[J]. 计算机学报,2013,36(6):1177-1182

[12] 李乔,郑啸. 云计算研究现状综述[J]. 计算机科学,2011,38(4): 32-37