Website：ycyk.brit.com.cn

适用于天地一体化网络的无证书密钥协商协议

于 勇[1]，郑鉴学[1]，张瑞嵩[1]，何亚光[2]，徐松艳[1]
（1. 北京遥测技术研究所 北京 100076；
2. 中国人民解放军96901部队 北京 100094）

摘要：为了保证天地一体化网络中用户信息的传输安全，改进传统方案的高时延等问题，本文提出一种轻量级的无证书密钥协商方案。首先，本文分析无证书密钥协商协议系统模型，针对天地一体化网络的特点提出协议需要满足双向认证、抗重放、完整性等安全需求。其次，本文选择一种轻量级的无证书加密方案，在此基础上提出密钥协商协议，满足天地一体化网络的资源和安全要求。最终，本文对提出的密钥协商协议进行BAN（Burrow-Adadi-Needham）逻辑安全性分析，并结合软件对协议性能仿真进行比较，结果表明：该方案在满足网络安全性需求的同时实现高效快速的协商。

关键词：无证书密钥协商；BAN逻辑；天地一体化网络；轻量级密码协议
中图分类号：V556.1; TN953 **文献标志码：**A **文章编号：**2095-1000(2024)01-0031-07
DOI：10.12347/j.ycyk.20230927001
引用格式：于勇，郑鉴学，张瑞嵩，等. 适用于天地一体化网络的无证书密钥协商协议[J]. 遥测遥控，2024，45(1)：31–37.

A Certificateless Key Agreement Protocol for the Integrated Network of Space and Ground

YU Yong[1]，ZHENG Jianxue[1]，ZHANG Ruisong[1]，He Yaguang[2]，XU Songyan[1]
（1. Beijing Research Institute of Telemetry，Beijing 100076，China；
2. 96901 Troops，PLA，Beijing 100094，China）

Abstract: In order to ensure the communication security of users and improve the high latency of traditional solutions in the integrated network of space and ground. In this paper, we propose a lightweight certificateless key agreement scheme. Firstly, we analyze the certificateless key agreement protocol system model. Based on the characteristics of the integrated network of space and ground, it is proposed that the protocol needs to satisfy some security requirements such as two-way authentication, anti-replay, and integrity. Then, we choose a lightweight certificateless encryption scheme. Base on the encryption scheme, we propose a key agreement protocol to meet the resource and security requirements of the integrated network of space and earth. Finally, we prove the proposed key agreement protocol security conducted on the BAN logical analysis, and compare the protocol performance with software simulation. The results show that the solution not only meets the network security requirements, but also provides fast and efficient negotiation.

Keywords: Certificateless key agreement scheme; BAN logical analysis; Integrated network of space and ground; lightweight encryption
Citation: YU Yong, ZHENG Jianxue, ZHANG Ruisong, et al. A Certificateless Key Agreement Protocol for the Integrated Network of Space and Ground[J]. Journal of Telemetry, Tracking and Command, 2024, 45(1): 31–37.

0 引言

传统网络的密钥协商研究技术已经非常成熟，但大多数需要进行复杂的密码学运算，并且交互次数频繁。这些方案无法直接结合天地一体化网络特点使用，虽有部分学者针对网络特点设计了合适的密钥协商方案[1-9]，Cruickshank[3]等结合天地一体化网络特点设计了基于公钥体制的认证方法，用户和卫星能够进行双向认证，但是效率不高且未考虑重复接入的问题，并且不具有匿名性。

收稿日期：2023-09-27；修回日期：2023-11-01

Hwang[4]等对上述方案加以改进，设计了适用于卫星通信系统的认证方法，但是降低了计算开销，不具备前向安全。Bao[9]等提出的基于身份的跨域密钥协商协议使用了双线性映射，能够快速高效认证，降低了存储和通信开销，但是计算开销增加。这些方案基本上都包含可信第三方的参与，需要进行多次的星地交互，这会带来高传输时延，进而影响服务质量。因此，为了保证天地一体化网络中用户信息的传输安全，解决传统方案的高时延等问题，需要设计一种轻量级的密钥协商方案。

由于网络规模持续增大，用户节点数也愈多，若只使用对称密码体制进行密钥协商协议，将会带来大量的密钥存储问题，而传统公钥体制需要可信第三方管理证书，存储和计算开销也随之增加，易造成单点访问瓶颈，不适用于资源受限的网络。Shamir[10]提出的基于身份的公钥体制无需证书管理，但存在密钥托管问题。Al-Riyami 和 Paterson[11]为了解决密钥托管和证书管理问题，提出了无证书公钥密码（Certificateless Public Key Cryptography，CL-PKC），它的特性适合用于天地一体化网络中。基于无证书密码系统协商方案，REN[12]等提出的加密认证方案降低了通信开销，但是计算开销却大大提升，效率降低。Chen[13]等为了减少用户计算开销，提出的高效认证协议只需进行哈希和异或运算，但是无法抵抗中间人攻击。

因此，本文针对上述问题，结合天地一体化网络特点提出了无证书的密钥协商协议，显著降低了通信开销和计算开销，协商过程中无需可信第三方参与，且仅需三次交互就能够完成密钥协商，降低了传输时延。通信双方只需执行哈希、异或和椭圆曲线上的点运算，降低了计算开销。随后对协议进行形式化分析，证明本协议能够满足天地一体化网络安全需求。最后使用软件仿真，证明协议的实用性。

1 系统模型与安全需求

结合天地一体化网络特点[14-16]，基于无证书密钥协商协议的模型如图 1 所示，系统包含用户、卫星及中心站。其中，用户作为协商的发起方，是具有卫星通信功能的终端。卫星作为协商的接收方，与用户进行三次交互产生密钥。用户进行密钥协商之前首先需要在中心站进行身份注册，生成自身公私钥对。中心站在初始化阶段负责整个系统参数的生成、用户密钥的协商、卫星密钥的分发以及后续阶段密钥的管理，不参与用户和卫星的密钥协商过程。

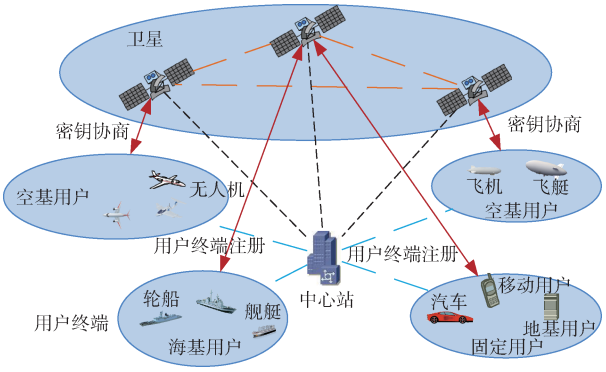

图 1 无证书密钥协商协议系统模型

Fig. 1 The system model of certificatless key agreement protocol

本模型中的中心站是被认为完全可信的，在整个流程中控制器不参与，视为可信的转发者，只负责将消息进行转发，不参与协议的交互。

若用户不具有卫星通信功能，则它与卫星通信需要控制器进行转发，固定用户通过有线方式发送给地面控制器，移动用户可通过无线方式发送给地面控制器或空间控制器，由控制器制定相应路由策略发送到通信接收卫星。卫星返回消息给用户也是如此。

结合天地一体化网络的特点，本节提出协议需要满足的安全需求如下：

① 双向认证性：用户和卫星之间能够完成双向认证，攻击者无法假冒任何一方从而协商出密钥。

② 抗重放攻击：协议保证用户和卫星的交互消息被截获后，即使被重放也无法协商密钥。

③ 完整性：消息在传输时若遭到篡改，则参与方无法正确协商出密钥。

2 无证书密钥协商协议设计

传统无证书密钥协商协议普遍使用椭圆曲线加密算法来实现用户的双向认证和密钥协商，但是传统加密算法存在计算复杂、密文较长等问题，若基于传统无证书加密方案设计协议，则会带来身份认证时间长、计算开销大等问题。因此首先需要选择一种轻量级的无证书加密方案，在此基础上设计密钥协商协议能更好地满足天地一体化

网络的资源和安全要求。

2.1　BSNS-CLPKE 方案

2005 年，Bake[17]等提出了基于 Schnorr 签名的 π 无证书加密方案，该方案不需要双线性对运算，且满足目前的强安全需求，方案概述如下：

① 系统建立

私钥生成中心(Private Key Generator，PKG)对于安全参数 k，产生两个大素数 p、q，且满足 $q|p-1$。

产生 Z_p^* 上的生成元 g，随机选择 $x\in Z_q^*$ 作为系统的主私钥，计算 $y=g^x$ 作为系统主公钥。

产生杂凑函数如下：

$H_1:\{0,1\}^*\times Z_p^*\to Z_q^*$，

$H_2:\{0,1\}^*\times Z_p^*\times Z_p^*\to Z_q^*$，

$H_3:\{0,1\}^*\to Z_q^*$，$H_4:Z_p^*\times Z_p^*\to\{0,1\}^{n+k_0}$，

其中，n 和 k_0 分别是明文和随机数的比特长度。

最后产生系统公共参数

$params=\{p,q,g,y,H_1,H_2,H_3,H_4\}$。

② 部分私钥产生

对于给定的身份 ID，PKG 随机选择 $s_0,s_1\in_R Z_q^*$，计算 $w_0=g^{s_0}$，$w_1=g^{s_1}$，$d_0=s_0+xH_1(ID,w_0)$，$d_1=s_1+xH_2(ID,w_0,w_1)$，返回用户部分私钥 $D_{ID}=d_0$，部分公钥 $P_{ID}=(w_0,w_1,d_1)$。

③ 秘密值产生

实体用户 ID 选择 $z\in_R Z_q^*$，返回 $s_{ID}=z$。

④ 私钥产生

实体用户 ID 输入 (D_{ID},s_{ID})，返回用户的完整私钥 $SK_{ID}=(d_0,z)$。

⑤ 公钥产生

输入 (P_{ID},s_{ID})，计算 $u=g^z$，返回用户的完整公钥 $PK_{ID}=(u,w_0,w_1,d_1)$。

⑥ 加密

假设消息的比特长度是 n，分解用户的公钥 $PK_{ID}=(u,w_0,w_1,d_1)$。判断等式 $g^{d_1}=w_1y^{H_2(ID,w_0,w_1)}$，若相等，随机选择 $\sigma\in_R\{0,1\}^{k_0}$，计算 $r=H_3(M,\sigma,ID,u)$，$U=g^r$，$V=(M||\sigma)\oplus H_4(w_0{}^r y^{H_1(ID,w_0)r},u^r)$，输出密文 $C=(U,V)$。

⑦ 解密

分解密文消息 $C=(U,V)$，用户私钥 $SK_{ID}=(d_0,z)$。

计算 $(M||\sigma)=V\oplus H_4(U^{d_0},U^z)$，$r=H_3(M,\sigma,ID,u)$，若 $g^r=U$，返回明文 M，否则解密失败。

2.2　无证书密钥协商协议流程

结合上述方案，本节对该加密方案进行修改，在此基础上提出了一个无证书密钥协商协议，该协议运行在椭圆曲线上。假设参与双方为用户 A 和卫星 B，其身份信息分别是 ID_A 和 ID_B，协议包含系统参数生成阶段、用户密钥生成阶段和密钥协商阶段。

① 系统参数生成

PKG 对于安全参数 k，产生大素数 q。

选取椭圆曲线上点的 P 是阶为 q 的循环群 G 的生成元，随机选择 $x\in Z_q^*$ 作为系统的主私钥，计算 $y=xP$ 作为系统主公钥。

产生杂凑函数如下：

$$H_1:\{0,1\}^*\times G\to Z_q^*,H_2:\{0,1\}^*\times G\times G\times G\times G\to Z_q^*,$$
$$H_3:\{0,1\}^*\to\{0,1\}^k$$

最终公开系统参数 $params=\{q,P,Y,H_1,H_2,H_3\}$

② 用户密钥生成

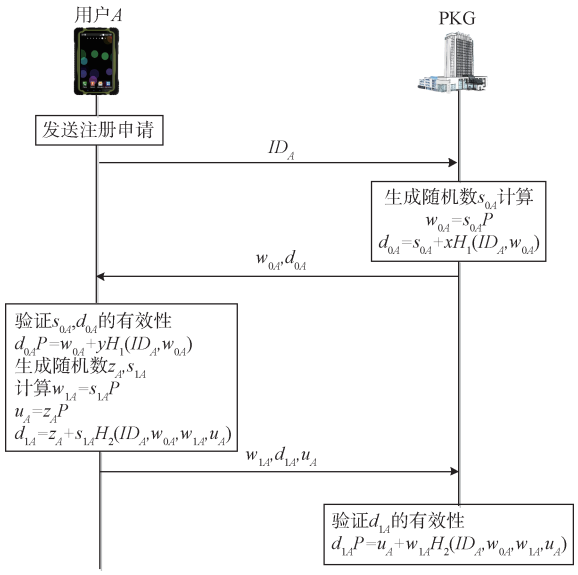

图 2　注册流程

Fig. 2　The flow of registration

用户密钥生成的具体过程如图 2 所示，相关描述如下：

用户 A 首先发送身份标识 ID_A 给 PKG。PKG 收到后，判断 ID_A 的合法性，若 ID_A 不是合法且未注册过的用户，拒绝服务请求，否则同意用户的注册请求，随机选择 $s_{0A}\in Z_q^*$，计算 $w_{0A}=s_{0A}P$，$d_{0A}=s_{0A}+xH_1(ID_A,w_{0A})$，$w_{0A}$ 为用户的部分公钥，d_{0A} 为用户的部分私钥，发送 (w_{0A},d_{0A}) 给用户 A。

用户 A 收到 PKG 返回的信息后，首先利用

PKG 的公钥 y 和接收的信息 (w_{0A}, d_{0A}) 验证等式 $d_{0A}P = w_{0A} + yH_1(ID_A, w_{0A})$ 是否成立，若不成立，则此消息不是合法 PKG 产生，丢弃会话并重新发送注册请求；若成立，则随机选择 $z_A, s_{1A} \in Z_q^*$，计算 $w_{1A} = s_{1A}P$，$u_A = z_A P$，$d_{1A} = z_A + s_{1A}H_2(ID_A, w_{0A}, w_{1A}, u_A)$，发送 (w_{1A}, d_{1A}, u_A) 给 PKG，则 (w_{1A}, u_A) 是用户产生的秘密值，d_{1A} 为用户 A 产生的公开参数，用户 A 的私钥包含 PKG 产生的部分私钥和用户本身产生的秘密值，即为 (s_{1A}, d_{0A}, z_A)。

PKG 接收到信息后，通过判断等式 $d_{1A}P = u_A + w_{1A}H_2(ID_A, w_{0A}, w_{1A}, u_A)$ 是否成立来验证用户 A 的公开参数 d_{1A} 的合法性，若成立，则保存 d_{1A} 为用户的公钥分量，并公开用户的公钥为 $(w_{1A}, w_{0A}, d_{1A}, u_A)$。

③ 密钥协商

在此阶段，本协议通过三次信息交互完成了用户 A 和卫星 B 之间的双向认证，并且生成了会话密钥 SK，方案流程如图 3 所示：

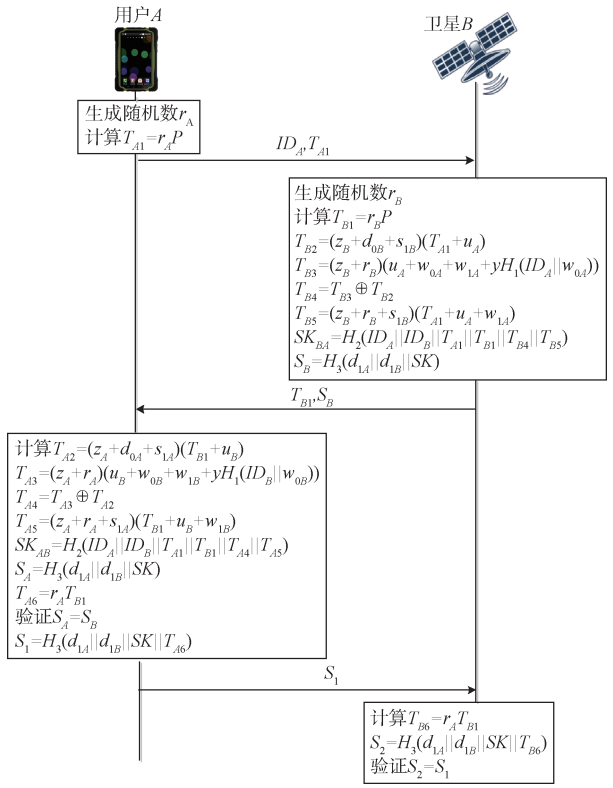

图 3 密钥协商流程

Fig. 3 The flow of key agreement

详细描述如下：

用户 A 随机选择 $r_A \in Z_q^*$，计算 $T_{A1} = r_A P$，并和自身标识一同 (ID_A, T_{A1}) 发送给卫星 B。

卫星 B 收到消息后，随机选择 $r_B \in Z_q^*$，计算 $T_{B1} = r_B P$。根据 ID_A 分解用户 A 公钥为 $(w_{1A}, w_{0A}, d_{1A}, u_A)$，分解自身私钥为 (s_{1B}, d_{0B}, z_B)，利用用户 A 公钥和自身私钥进行如下计算：

$$\begin{aligned}
&T_{B2} = (z_B + d_{0B} + s_{1B})(T_{A1} + u_A)\\
&T_{B3} = (r_B + z_B)(u_A + w_{0A} + w_{1A} + yH_1(ID_A||w_{0A}))\\
&T_{B4} = T_{B2} \oplus T_{B3}\\
&T_{B5} = (r_B + z_B + s_{1B})(T_{A1} + u_A + w_{1A})\\
&SK_{BA} = H_2(ID_A||ID_B||T_{A1}||T_{B1}||T_{B4}||T_{B5})\\
&S_B = H_3(d_{1A}||d_{1B}||SK)
\end{aligned} \tag{1}$$

发送 (T_{B1}, S_B) 给用户 A。

用户 A 收到信息后，分解卫星 B 公钥为 $(w_{1B}, w_{0B}, d_{1B}, u_B)$，分解自身私钥为 (s_{1A}, d_{0A}, z_A)，进行如下计算：

$$\begin{aligned}
&T_{A2} = (r_A + z_A)(u_B + W_{1B} + W_{0B} + yH_1(ID_B||W_{0B}))\\
&T_{A3} = (z_A + d_{0A} + s_{1A})(T_{B1} + u_B)\\
&T_{A4} = T_{A2} \oplus T_{A3}\\
&T_{A5} = (r_A + z_A + S_{1A})(u_B + T_{B1} + W_{1B})\\
&SK_{AB} = H_2(ID_A||ID_B||T_{A1}||T_{B1}||T_{A4}||T_{A5})\\
&S_A = H_3(d_{1A}||d_{1B}||SK)
\end{aligned} \tag{2}$$

验证 S_A 和 S_B 是否相等，若不相等，则会话密钥协商失败，否则计算 $T_{A6} = r_A T_{B1}$，$S_1 = H_3(d_{1A}||d_{1B}||SK||T_{A6})$，发送 S_1 给卫星 B。

卫星 B 接收到消息后，计算 $T_{B6} = r_B T_{A1}$，$S_2 = H_3(d_{1A}||d_{1B}||SK||T_{B6})$，验证 S_1 和 S_2 是否相等，若相等，则协商成功，SK 为此次会话协商的密钥。

3 协议分析

3.1 正确性分析

可以验证双方计算的密钥是相等的：

$$\begin{aligned}
T_{A2} &= (r_A + z_A)(u_B + W_{1B} + W_{0B} + yH_1(ID_B||W_{0B}))\\
&= (r_A + z_A)(z_B P + S_{1B}P + d_{0B}P)\\
&= (r_A P + z_A P)(z_B + S_{1B} + d_{0B})\\
&= (T_{A1} + u_A)(z_B + d_{0B} + S_{1B})\\
&= T_{B2}
\end{aligned} \tag{3}$$

同理，$T_{A3} = T_{B3}$，所以 $T_{A4} = T_{B4}$。

$$\begin{aligned}
T_{A5} &= (r_A + z_A + S_{1A})(u_B + T_{B1} + W_{1B}) =\\
&(r_A + z_A + S_{1A})(z_B P + r_B P + S_{1B}P) =\\
&(r_A P + z_A P + S_{1A}P)(z_B P + r_B + S_{1B}) =\\
&(T_{A1} + u_A + W_{1A})(r_B + z_B + S_{1B}) = T_{B5}
\end{aligned} \tag{4}$$

通过上述等式，能够得到 $SK_{AB} = SK_{BA}$，因此本协议会话协商能够保证密钥的一致性。

3.2 安全性分析

BAN 逻辑是最为广泛使用的形式化逻辑分析

方法，其通过证明密码协议参与方之间的可信认证，辅以逻辑推理对协议进行证明，在身份认证和密钥协商协议中起着重要的作用，能够分析协议在通信参与实体中是否能协商出秘密的会话密钥。

因此，基于BAN逻辑分析本章提出的协议过程如下：首先列出协议最终需要满足的安全目标；其次，对协议的状态初始化、传输信息理想化；最后，结合BAN逻辑的规则进行推导，分析是否能够满足安全目标。

结合BAN逻辑标识定义和含义，协议证明过程如下：

① 安全目标：

G_1:$A|\equiv A\xleftrightarrow{SK}B$，主体$A$相信，$SK$是主体$A$和$B$的秘密共享密钥，仅被$A$，$B$所知。

G_2:$B|\equiv B\xleftrightarrow{SK}A$，主体$B$相信，$SK$是主体$A$和$B$的秘密共享密钥，仅被$A$，$B$所知。

② 协议理想的初始化状态：

A_1:$B|\equiv\#(T_{A1})$，主体B相信，消息T_{A1}是新鲜的，此之前未被发送过。

A_2:$A|\equiv\#(T_{B1})$，主体A相信，消息T_{A1}是新鲜的，此之前未被发送过。

A_3:$A|\equiv(\xrightarrow{u_B}B)$，主体$A$相信，$u_B$是主体$B$的公钥。

A_4:$A|\equiv(\xrightarrow{w_{0B}}B)$，主体$A$相信，$w_{0B}$是由PKG颁发给主体$B$的公钥。

A_5:$A|\equiv(\xrightarrow{w_{1B}}B)$;

A_6:$A|\equiv(\xrightarrow{d_{1B}}B)$，主体$A$相信，$w_{1B}$，$d_{1B}$是主体$B$的公开值。

A_7:$B|\equiv(\xrightarrow{u_A}A)$，主体$B$相信，$u_A$是主体$A$的公钥。

A_8:$B|\equiv(\xrightarrow{w_{0A}}A)$，主体$B$相信，$w_{0A}$是由PKG颁发给主体$A$的公钥。

A_9:$B|\equiv(\xrightarrow{w_{1A}}A)$;

A_{10}:$B|\equiv(\xrightarrow{d_{1A}}A)$，主体$B$相信，$w_{1A}$，$d_{1A}$是主体$A$的公开值。

A_{11}:$A|\equiv B\Rightarrow(z_B,d_{0B},s_{1B})$，主体$A$相信，主体$B$拥有秘密值$z_B,d_{0B},s_{1B}$。

A_{12}:$B|\equiv A\Rightarrow(z_A,d_{0A},s_{1A})$，主体$B$相信，主体$A$拥有秘密值$z_A,d_{0A},s_{1A}$。

A_{13}:$B|\equiv A\Rightarrow(T_{A1})$，主体$B$相信，$T_{A1}$是主体$A$发送的消息。

A_{14}:$A|\equiv B\Rightarrow(T_{B1})$，主体$A$相信，$T_{B1}$是主体$\boldsymbol{B}$发送的消息。

③ 协议理想化：

本文协议传递的3条消息，形式化语言描述如下：

$$M_1:A\rightarrow B:(T_{A1})$$

$$M_2:B\rightarrow A:(T_{B1},\{d_{1A},d_{1B},\{<T_{A1},u_A,w_{1A}>\}_{<z_B,d_{0B},s_{1B}>}\}_{\{T_{B1}\}_{T_{A1}}})$$

$$M_3:A\rightarrow B:(T_{A1},\{d_{1A},d_{1B},\{<T_{B1},u_B,w_{1B}>\}_{<z_A,d_{0A},s_{1A}>}\}_{\{T_{A1}\}_{T_{B1}}})$$

④ 证明推导：

根据M_1可得：

S_1:$B\triangleleft(T_{A1})$，主体B收到消息M_1。

根据M_2可得：

S_2:$A\triangleleft(T_{B1},\{d_{1A},d_{1B},\{<T_{A1},u_A,w_{1A}>\}_{<z_B,s_{1B}>}\}_{\{T_{B1}\}_{T_{A1}}})$，主体$A$收到消息$M_2$。

根据M_3可得：

S_3:$B\triangleleft(T_{A1},\{d_{1A},d_{1B},\{<T_{B1},u_B,w_{1B}>\}_{<z_A,s_{1A}>}\}_{\{T_{A1}\}_{T_{B1}}})$，主体$B$收到消息$M_3$。

根据A_7，A_9，S_2和消息含义规则

$$\frac{P|\equiv\xleftrightarrow{K}Q,P\triangleleft\{X\}_K}{P|\equiv Q|\sim X}$$

可得：

S_4:$B|\equiv A|\sim(T_{A1},u_A,w_{1A})$，主体$B$相信，主体$A$之前某个时刻发送过消息$T_{A1},u_A,w_{1A}$。

根据A_3，A_5，S_3和消息含义规则，可得：

S_5:$A|\equiv B|\sim(T_{B1},u_B,w_{1B})$，主体$A$相信，主体$B$之前某个时刻发送过消息$T_{A1},u_A,w_{1A}$。

根据S_4，A_1和临时值验证规则

$$\frac{P|\equiv\#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$$

可得：

S_6:$B|\equiv A|\equiv T_{A1}$，主体B相信，主体A相信T_{A1}。

根据S_5，A_2和临时值验证规则

$$\frac{P|\equiv\#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$$

可得：

S_7:$A|\equiv B|\equiv T_{B1}$，主体A相信，主体B相信T_{B1}。

根据S_6，A_{13}和管辖权规则

$$\frac{P|\equiv Q|\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$$

可得：

S_8:$B|\equiv T_{A1}$，主体 B 相信 T_{A1}。

根据 S_7，A_{14} 和管辖权规则，可得：

S_9:$A|\equiv T_{B1}$，主体 A 相信 T_{B1}。

根据 A_1 和新鲜性规则 $\dfrac{P|\equiv\#(X)}{P|\equiv\#((X,Y))}$，可得：

S_{10}:$A|\equiv\#(SK_{BA})$，主体 A 相信，SK_{BA} 是新鲜的。

根据 A_2 和新鲜性规则，可得：

S_{11}:$B|\equiv\#(SK_{AB})$，主体 B 相信，SK_{AB} 是新鲜的。

根据 S_{10}，S_6 和会话密钥规则

$$\frac{P|\equiv\#(X),P|\equiv Q|\equiv X}{P|\equiv P\overset{SK}{\longleftrightarrow}Q}$$

可得：

$A|\equiv A\overset{SK}{\longleftrightarrow}B$，满足目标 G_1

根据 S_{11}，S_7 和会话密钥规则，可得：

$B|\equiv B\overset{SK}{\longleftrightarrow}A$，满足目标 G_2

通过基于BAN逻辑的形式化分析，能够证明本协议可以满足安全目标。这意味着本协议可以实现双向认证和秘密协商出会话密钥。

3.3　性能分析

将一次群上的乘法运算记作 M，一次数字签名运算记作 S，L_G 表示群中元素的长度，L_z 表示 Z_q^* 中元素的长度，L_S 表示签名的长度，本文方案与现有相关方案的效率比较表见表1。

表 1　性能分析

Table 1　The performance analysis

协议	计算开销	消息长度	交互次数
文献[18]	$7M$	$2L_G+2L_z$	3
文献[19]	$2M+2S$	L_G+L_S	4
本文协议	$5M$	L_G+L_z	3

从上表中可以看出，本文的交互次数少，密钥协商在第二步就可完成，第三步是为了保证通信双方的认证性。消息长度短，并且计算开销少。

本文方案选用的NIST标准的Koblitz曲线K-233，主要是执行在有限域 $GF(2^{233})$ 中的各种运算，因此群元素的长度不超过462 bit，H_3 哈希值的信息长度不超过231 bit。假设在天地一体化与卫星通信的场景下[2]，相关参数见表2。

完成协议会产生的通信延迟大约为32 ms，其中接入网络延迟占比较大。所以本文的交互次数少，消息长度短，并且计算开销少，与文献[18,19]相比通信延迟较低。

本文的密钥协商协议在选型为Xilinx公司的Kintex-7型FPGA芯片，相应开发软件选择Vivado 2018.3，该软件在Windows 7操作系统环境下实现对协议仿真。仿真曲线选择NIST标准的Koblitz曲线K-233，最终协议运行耗费时间如表3所示：

表 2　模拟天地一体化网络环境参数设定

Table 2　The parameter settings of the integrated network of space and ground

参数	参数值
封装包大小	1 024 Bytes
协议仿真时间	0.75 ms
卫星最大带宽	1T bits/s
接入网络延迟	10 ms
卫星覆盖面积	30×10^4 km^2

表 3　运行时间

Table 3　The runtime analysis

运算	模乘	点加	点乘	协议运行
运行时间(μs)	0.09	0.77	159	752

由于在密钥协商协议的所有运算中，点乘运算耗费时间最久，并且包含了点加和模乘运算，所以协议运行的速度主要取决于点乘运算的花费时间。点乘运算的性能比较图，如图4所示。

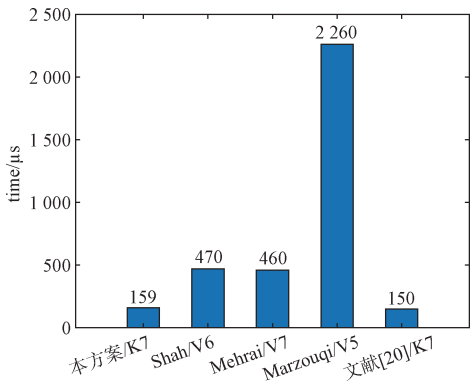

图 4　点乘性能比较图

Fig. 4　The comparison of dot product runtime

本文点乘运算采用滑动窗法，从图4可以看出，该点乘运行耗费时间较少，因此密钥协商协议能够在较短时间内协商出密钥，满足天地一体化网络的需求。

4　结束语

本文针对传统天地一体化网络密钥协商交互次数多、通信开销大等问题，提出了一种基于无证书的协商协议，该协议基于改进的轻量级无证

书加密方案，用户和卫星交互次数仅为三次，信息传输内容最多为椭圆曲线点与哈希值的比特长度，通信开销小，双方计算仅使用椭圆曲线点运算和哈希运算，计算开销小。最后使用BAN逻辑对协议进行安全性分析，并结合软件仿真对协议性能进行比较，结果表明方案在满足网络安全性需求的同时提供高效快速的协商。

参考文献

[1] 孟薇 . 天地一体化信息网络安全接入认证机制研究[D]. 合肥: 中国科学技术大学,2019

[2] 刘子琦 . 天地一体化网络安全接入认证方案设计与实现[D]. 重庆: 重庆邮电大学,2020.

[3] CRUICKSHANK H.S. A security system for satellite networks[C]//The Fifth International Conference on Satellite Systems for Mobile Communications and Navigation, London. UK.IET, 1996:187-190.

[4] HWANG M S, YANG C C, SHIU C Y. An authentication scheme for mobile satellite communication systems[J]. ACM SIGOPS Operating Systems Review, 2003, 37(4): 42-47.

[5] 张民, 罗光春, 王俊峰, 等 . 空间信息网络可靠传输协议研究[J]. 通信学报, 2008, 29(6): 63-68.
ZHANG Min, LUO Guangchun, WANG Junfeng, et al. Reliable transmission control protocol for spatial information networks[J]. Journal on Communications, 2008, 29(6): 63-68.

[6] HE D, CHEN C, CHAN S, et al. Secure and efficient handover authentication based on bilinear pairing functions[J]. IEEE Transactions on Wireless Communications,2012 ,11(1):48-53.

[7] LI X, ZHANG Y, LIU X, et al. A lightweight roaming authentication protocol for anonymous wireless communication[C]//Global Communications Conference. IEEE, 2012: 1029-1034.

[8] CAO J, MA M, LI H. A group-based authentication and key agreement for MTC in LTE networks[C]//Global Communications Conference (GLOBECOM). IEEE, 2012.

[9] BAO BAO Q, HOU M, CHOO K K R. A one-pass identity-based authentication and key agreement protocol for wireless Roaming[C]//The Sixth International Conference on Information Science and Technology. IEEE, 2016: 443-447.

[10] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Proceedings of the CRYPTO'84, Lecture Notes in Computer Science 196. Berlin:Springer-Verlag, 1984: 47-53.

[11] AL-RIYAMI S S,PATERSON K G. Certificateless public key cryptography[C]//Advances in Cryptology ASIACRYPT 2003. Heidelberg: Springer Berlin, 2003: 452-473.

[12] REN F,MA J F, HAO X W. Certificate-based hybrid public key infrastructure for space information networks[J]. Jilin Daxue Xuebao (Gongxueban)/Joumal of Jilin University (Engineering and Technology Edition), 2012, 42(2): 440-445.

[13] CHEN T H,LEE W B,CHEN H B. A self-verification authentication mechanism for mobile satellite communication systems[J]. Computers & Electrical Engineering, 2009, 35(1): 41-48.

[14] 李凤华, 殷丽华, 吴巍, 等 . 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报, 2016(11): 156-168.
LI Fenghua, YIN Lihua, WU Wei, et al. Research status and development trends of security assurance for space-ground integration information network[J]. Journal on Communications, 2016(11): 156-168.

[15] 吴曼青, 吴巍, 周彬, 等 . 天地一体化信息网络总体架构设想[J]. 卫星与网络, 2016, 158(3): 30-36.

[16] 沈荣骏 . 我国天地一体化航天互联网构想[J]. 中国工程科学, 2006(10): 19-30.

[17] BAEK J., SAFAVI-NAINI R. Certifieateless public key encryption without pairing[C]//Proc. of the 8th International Conference on Information Security(ISCZoos), Springer Verilag, 2005: 134-148,

[18] 莫天庆, 何咏梅 . 一种基于无证书的SIP认证密钥协商协议[J]. 计算机科学, 2020, 47(6A): 413-419.
MO Tianqing, HE Yongmei. SIP authentication key agreement of protocol base on certificateless[J]. Computer Science, 2020, 47(6A): 413-419.

[19] NI L. Research on some issues in authenticated key agreement protocols[D]. Shanghai: Shanghai Jiao Tong University,2012.

[20] YANG G Q, KONG F Y, XU Q L. Optimized FPGA implementation of elliptic curve cryptosystem over prime fields[C]//International conference on trust, security and privacy in computing and communications (Trust Com). IEEE, 2020: 243-249.

[作者简介]

于　勇　1970年生，博士，研究员。

郑鉴学　1998年生，硕士研究生。

张瑞嵩　1998年生，硕士研究生。

何亚光　1973年生，硕士，副研究员。

徐松艳　1978年生，硕士，研究员。

(本文编辑：潘三英)