Website：ycyk.brit.com.cn

空间信息网络公钥管理方案的设计与分析

杨静春[1]，陈韬鸣[2]，蒋　鑫[1]，徐松艳[1]，张道法[1]
（1 北京遥测技术研究所 北京 100076；
2 北京跟踪与通信技术研究所 北京 100094）

摘要：为保障空间信息网络认证与密钥分发的安全性，本文提出了一种基于椭圆曲线密码系统的公钥管理方案，提供入网认证、密钥协商和密钥更新等功能，实现了认证性、抗重放和前向/后向安全性等多种安全目标。对于卫星间的认证和密钥协商，本方案仅需卫星之间进行3次交互即可完成。通过对方案进行安全性和效率分析，证实了本方案在空间信息网络中的实际可用性以及同现有公钥管理方案相比效率上的优越性。

关键词：空间信息网络；公钥管理；认证和密钥协商；椭圆曲线密码系统
中图分类号：V556.1；TN918　　**文献标志码：**A　　**文章编号：**2095-1000(2024)05-0050-08
DOI：10.12347/j.ycyk.20240412002
引用格式：杨静春，陈韬鸣，蒋鑫，等. 空间信息网络公钥管理方案的设计与分析[J]. 遥测遥控，2024，45(5)：50–57.

Design and Analysis of The Public-key Management Scheme for The Space Information Network

YANG Jingchun[1]，CHEN Taoming[2]，JIANG Xin[1]，XU Songyan[1]，ZHANG Daofa[1]
（1. Beijing Research Institute of Telemetry, Beijing 100076, China;
2. Beijing Institute of Tracking and Telecommunications Technology, Beijing 100094, China）

Abstract: To ensure the security of authentication and key distribution in the space information network, this paper proposes a public-key management scheme based on the elliptic curve cryptosystem. With the capacity for network access authentication and key agreement/update, this scheme can achieve various security goals, such as authenticity, anti-replay, and forward/backward security. For interstellar authentication and key agreement, our scheme only requires 3 interactions between the satellites. We provide a security and efficiency analysis for our scheme, and show that the proposed scheme not only satisfies the actual availability in the space information network, but also performs better than other existing public-key management schemes.

Keywords: Space information network; Public-key management; Authentication and key agreement; Elliptic curve cryptosystem
Citation: YANG Jingchun, CHEN Taoming, JIANG Xin, et al. Design and Analysis of The Public-key Management Scheme for The Space Information Network[J]. Journal of Telemetry, Tracking and Command, 2024, 45(5): 50–57.

0　引言

空间信息网络（Space Information Network, SIN）是指以天基网络、地基网络等多种异构网络融合形成的天地信息互联互通的综合网络系统[1]。空间信息网络不仅包含卫星与地面控制中心的星地链路，也有不同轨道、不同业务、不同速率的多种卫星间互联的星间链路。空间信息网络具有高度自治能力，能够对信息进行自动化收集、处理和分析[2]，已被广泛应用于导航、通信、遥感等多种领域，具备了广阔的应用前景和经济价值。

和地面网络类似，空间信息网络同样需要一套高效安全的密钥管理方案，以保证信息在传输过程中的机密性、完整性以及真实性，保障星地网络和星间网络的通信安全并提供入网认证、密钥协商、信息加解密、密钥更新等功能。然而，空间信息网络的拓扑实时动态变化，相比地面网络，存在传输时延大、星上计算和存储资源受限、

基金项目：国防预研项目
收稿日期：2024-04-12；修回日期：2024-06-17

误码率高等不足。因此，从以上角度考虑，空间信息网络的密钥管理方案需要最小化密钥更新的代价，减少认证和密钥协商的时间和计算复杂度。当会话密钥协商结束，为了高效地保护大量数据传输的机密性，可以考虑用对称密码算法对数据进行保护。同时，为了减少网络中总的密钥量，应该考虑降低每个卫星上的密钥存储。

目前，地面网络的密钥管理方案主要分为对称密钥管理方案、公钥管理方案和二者混合的密钥管理方案。最为典型的对称密钥管理方案是Kerberos方案[3]，该方案是基于有密钥分发中心的多方密钥管理方案。尽管对称密码体制有着计算高效的优势，然而其局限性也十分明显，主要表现在密钥量太大。若每个用户要想和其他$n-1$个用户通信，那么就必须使用$n-1$个密钥，如此系统总的密钥量达到$n(n-1)/2$。另外，对称密码体制也存在密钥分发、鉴别认证和不可否认性的困难[4]。为了解决这些问题，公钥密码体制应运而生。典型的公钥密码体制包括RSA[5]、ElGamal[6]和椭圆曲线密码系统（Elliptic Curve Cryptosystem, ECC）[7,8]。混合密钥管理方案[9]结合使用了对称密码体制和公钥密码体制，并使用了公钥、主密钥和会话密钥的概念。根据网络的不同，会话密钥可以利用对称体制更新，也可以利用公钥体制更新。

针对空间信息网络，国内外研究团队先后提出了许多认证和密钥协商方案。文献[10]利用公钥密码体制提出了地面用户与卫星网络间的认证和密钥协商方案。该方案具有前向安全性，但无法保证用户身份信息的机密性，由于使用了数字签名，因此也不适用于计算资源受限的用户终端和卫星节点。为解决文献[10]的问题，文献[11]提出了移动场景下用户认证和加密的方案，该方案具有抗重放性，但不具有前向安全性。文献[12]提出了一种利用预置共享密钥实现端端认证的密钥管理方案，该方案通过结合使用公钥密码和对称密码达到了自我验证的效果，然而无法抵抗中间人攻击。文献[13]给出了一种带有随机数交互的认证方式，该方案基于离散对数问题和哈希函数的单向性。文献[14]提出了一种仅使用哈希函数的认证方案。由于只有哈希函数，其安全性存在缺陷。文献[15]针对文献[14]提出改进方案，然而该方案仍然只使用了哈希函数，安全性仍无法保证。文献[16]利用椭圆曲线密码系统的加密和签名算法，实现了适用于移动卫星通信的单向认证。文献[17]使用代理签名，对于空间信息网络提出了快速的身份认证方法，并且降低了卫星节点被攻击的可能性，但是由于使用了多次对称加密算法和签名算法，其运算开销也很大。文献[18]结合椭圆曲线密码算法和对称密码算法，提出了另一种空间信息网络认证方案。

根据以上分析，空间信息网络的密钥管理如果只采用对称或者哈希算法，计算效率优势明显，但是安全性会降低。本文采用了基于椭圆曲线密码系统的公钥管理方案，完成卫星与地面控制中心的认证、卫星与卫星之间的认证以及密钥协商。为尽可能减少通信代价和计算量，本方案对于卫星间的认证和密钥协商无需地面控制中心参与，仅需3次交互即可完成。通过对方案进行安全性和效率分析，证实了本方案的实际可用性和效率上的优越性。

1　椭圆曲线密码系统

1985年，美国学者Koblitz[7]和Miller[8]分别独立地提出了基于椭圆曲线的密码系统。对于有限域GF(p)上的椭圆曲线，线上所有点加上无穷远点可以构成一个有限交换加法群，在这个群上可以定义离散对数系统，椭圆曲线密码系统正是在这个群上定义的一类公钥密码系统。

1.1　有限域上的椭圆曲线

密码学领域经常使用的一类有限域上的椭圆曲线为E：$y^2\equiv x^3+ax+b(\mathrm{mod}\,p)$。这里，$p$是一个很大的素数，$a,b,x$和$y$都定义在有限域GF($p$)=$\{0,1,\cdots,p-1\}$上，并且满足$4a^3+27b^2(\mathrm{mod}\,p)\neq 0$。有限域上椭圆曲线群$E_p(a,b)$里的元素包括所有在曲线上的点$(x,y)$和一个无穷远点$O$。

1.2　椭圆曲线上点的加法和乘法

对于椭圆曲线群$E_p(a,b)$中无穷远点O和椭圆曲线上任意两个点$P=(x_1,y_1)$，$Q=(x_2,y_2)$，曲线群中的加法规则如下：

① $O+O=O$；

② $P+O=O+P=P$；

③ $P+(-P)=O$，$-P=(x_1,-y_1)$；

④ 如果$P\neq -Q$，则$P+Q=R=(x_3,y_3)\in E_p(a,b)$，

其中：

$$x_3=\lambda^2-x_1-x_2, y_3=\lambda(x_1-x_3)-y_1 \tag{1}$$

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1} & P\neq Q\\ \dfrac{3x_1^2+a}{2y_1} & P=Q\end{cases} \tag{2}$$

⑤ 对任意三个曲线上的点 P、Q、R，有 $P+Q=Q+P, P+(Q+R)=(P+Q)+R$。

椭圆曲线群 $E_p(a,b)$ 中的乘法规则如下：

① 对于正整数 k，曲线群里的任意一点 P，有 $kP=P+P+\cdots+P$；

② 对于整数 s 和 t，曲线群里的任意一点 P，有 $(s+t)P=sP+tP, s(tP)=(st)P$。

1.3 ECC 密钥对生成

对于曲线群里的点 P，使 $nP=O$ 成立的最小正整数 n 定义为曲线群里的点 P 的阶。在椭圆曲线 E 上，任何可以生成曲线上所有点的点定义为 E 的生成元。

假设椭圆曲线群 $E_p(a,b)$ 上的点 P 为生成元，如果方程 $Q=kP$ 成立，即 Q 为 P 的倍点，并且倍数是小于 p 的正整数 k，则由 k 和 p 计算出 Q 是容易的，但由 P、Q 计算出 k 是困难的，这便是椭圆曲线上的离散对数问题。对于椭圆曲线密码系统，生成用户 B 的公私钥对的过程如下：

① 对于椭圆曲线 $E: y^2\equiv x^3+ax+b(\mathrm{mod}\,p)$，构造椭圆曲线群 $E_p(a,b)$；

② 在椭圆曲线群 $E_p(a,b)$ 中选择生成元 $G=(x_0,y_0)$，并且满足 $nG=O$ 的最小正整数 n 是一个很大的素数；

③ 选择一个小于 n 的正整数 n_B 作为用户 B 的私钥，则用户 B 的公钥为 $P_B=n_BG$，用户 B 的公开参数为 (E,n,G,P_B)。

2 空间信息网络公钥管理方案

2.1 空间信息网络拓扑

空间信息网络由一个地面控制中心和多个卫星轨道构成。每个卫星轨道上有多个卫星节点，地面控制中心与每个卫星节点存在星地链路，卫星节点之间存在星间链路。地面控制中心在注册阶段与所有的卫星节点进行交互，并与每个卫星节点共同生成该节点的公私钥对。轨道内的卫星节点可以与同一轨道的卫星节点进行通信，也可以与不同轨道的卫星节点通信，同一轨道内的卫星通信和不同轨道间的卫星通信采用相同的通信协议。两个卫星节点在通信之前需要进行认证与会话密钥协商。空间信息网络拓扑图如图 1 所示。

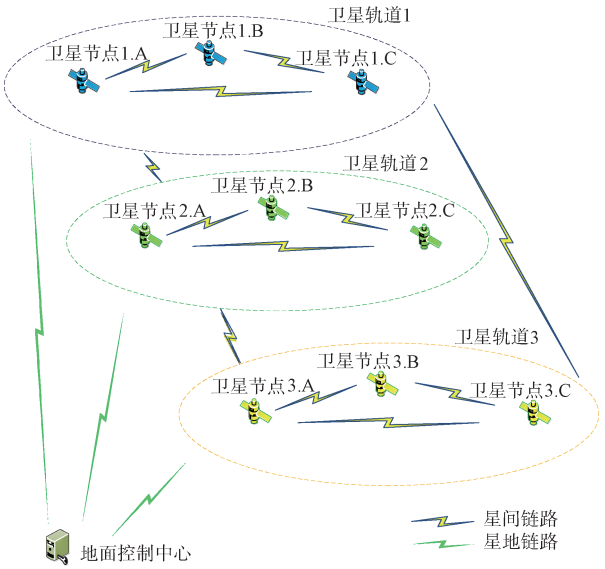

图 1 空间信息网络拓扑

Fig. 1 Topology of space information network

2.2 设置阶段

在设置阶段，地面控制中心为所有卫星节点配备系统的公开参数。公开参数包括以下内容：

① 有限域 GF(p) 上的椭圆曲线 E：$y^2\equiv x^3+ax+b(\mathrm{mod}\,p)$，这里 a 和 b 是常数，满足 $4a^3+27b^2(\mathrm{mod}\,p)\neq 0$，并且 GF($p$)$=\{0,1,\cdots,p-1\}$；

② 椭圆曲线的生成元 G（G 的阶为 n）；

③ 哈希函数 $H:\{0,1\}^*\rightarrow\{1,\cdots,n-1\}$；

④ 基于带密钥哈希函数的消息认证码算法 $KMAC:\{0,1\}^*\rightarrow\{0,1\}^m$，这里 m 是认证码的长度；

⑤ 基于哈希函数的密钥导出函数 $KDF:\{0,1\}^*\rightarrow\{0,1\}^k$，这里 k 是会话密钥的长度；

⑥ 地面控制中心的公钥 D。

这里，地面控制中心先选取自己的私钥 $d\in\{1,\cdots,n-1\}$，然后计算自己的公钥 $D=dG$。

2.3 注册阶段

在注册阶段，每个卫星节点和地面控制中心进行交互，共同生成该节点的公私钥对。与地面控制中心类似，每个卫星节点 i 先选取自己的部分私钥 $q_i\in\{1,\cdots,n-1\}$，然后计算自己的部分公钥

$Q_i=q_iG$。如图 2 所示。

第一步：卫星节点 i 计算部分身份认证信息 $T_i=(ID_i,Q_i)$(这里 ID_i 是卫星节点 i 的身份标识)，然后将 T_i 发给地面控制中心。

第二步：地面控制中心收到 T_i 后，为卫星节点 i 计算剩余部分私钥和剩余部分公钥。

① 地面控制中心首先选择一个随机数 $t_i\in\{1,\cdots,n-1\}$，然后计算椭圆曲线上的点 $R_i=t_iG$，并利用哈希函数计算 $h_i=H(T_i,R_i)$；

② 地面控制中心计算 $r_i=t_i+h_id\,(\mathrm{mod}\,n)$；

③ 地面控制中心把 r_i 作为卫星节点 i 的剩余部分私钥，把 R_i 作为卫星节点 i 的剩余部分公钥，然后把 r_i 和 R_i 发给卫星节点 i。

第三步：当卫星节点 i 收到 r_i 和 R_i 后，验证 $r_i\cdot G=R_i+h_i\cdot D$(因为 $r_i\cdot G=(t_i+h_id)\cdot G=t_i\cdot G+H(T_i,R_i)\cdot d\cdot G=R_i+h_i\cdot D$)。如果等式成立，说明 r_i 和 R_i 确实是由地面控制中心正确生成的。卫星节点 i 接着将自己生成的部分公私钥对和地面控制中心生成的剩余部分公私钥对合并，作为自己完整的公私钥对。卫星节点 i 的私钥为 $pri\_key_i=(q_i,r_i)$，公钥为 $pub\_key_i=(Q_i,R_i)$。

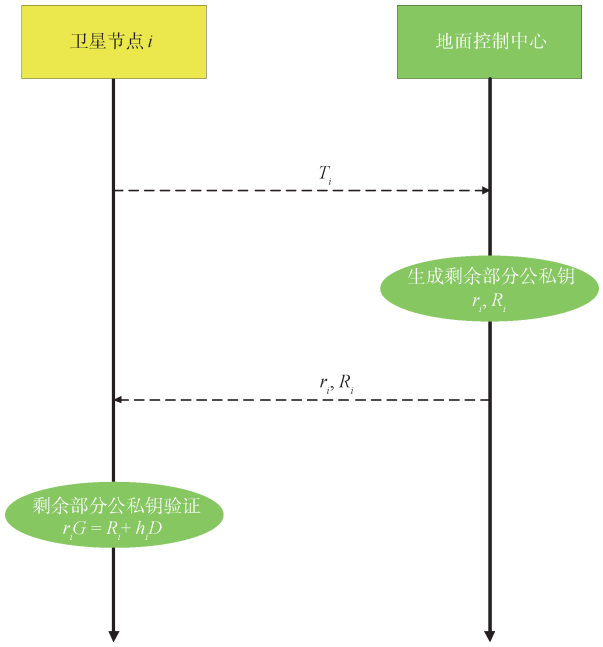

图 2　注册阶段的交互

Fig. 2　Interactions in registration phase

2.4　认证和密钥协商阶段

在注册阶段，每个卫星节点通过与地面控制中心交互，均生成了自己完整的公私钥对。当两个卫星节点 A 和 B 要进行通信时，需要使用设置阶段中预存的公开参数，以及双方在注册阶段中生成的公私钥对，通过执行认证和密钥协商协议，生成双方共有的会话密钥。把会话密钥作为对称密码算法(如高级加密标准 AES，Advanced Encryption Standard)的密钥，通过对明文消息加密，以及加密后的密文消息解密，可以建立 A 和 B 之间的安全通信。A 和 B 之间的认证和密钥协商过程如图 3 所示。

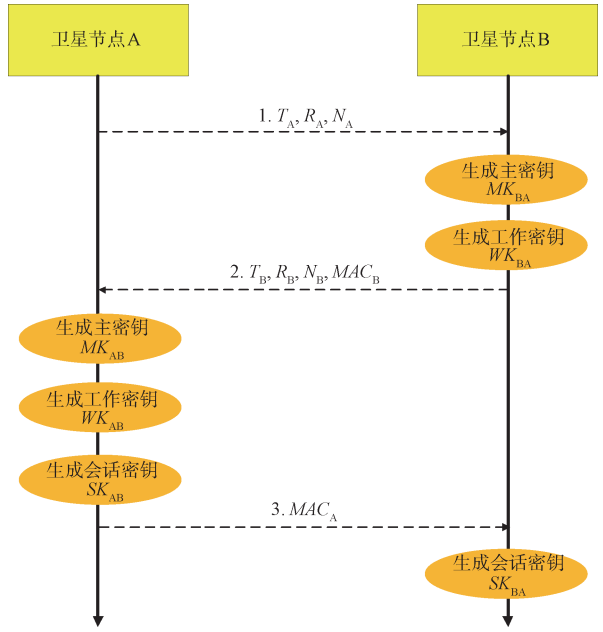

图 3　认证和密钥协商阶段的交互

Fig. 3　Interactions in authentication and key agreement phase

第一步：卫星节点 A 准备以下数据。

① 部分身份认证信息 $T_A=(ID_A,Q_A)$（这里 ID_A 是卫星节点 A 的身份标识，Q_A 是卫星节点 A 的部分公钥）；

② 剩余部分公钥 R_A；

③ 随机数 N_A，

然后卫星节点 A 将 T_A,R_A,N_A 发给卫星节点 B。

第二步：卫星节点 B 收到消息后，将收到的消息存储下来，然后准备以下数据。

① 部分身份认证信息 $T_B=(ID_B,Q_B)$（这里 ID_B 是卫星节点 B 的身份标识，Q_B 是卫星节点 B 的部分公钥）；

② 剩余部分公钥 R_B；

③ 随机数 N_B；

④ 利用哈希函数 H 计算主密钥 $MK_{BA}=\left(r_B\left(R_A+H(T_A,R_A)D\right),q_BQ_A\right)$；

⑤ 利用密钥导出函数 KDF 计算工作密钥 $WK_{BA}=KDF(MK_{BA})$；

⑥ 利用消息认证码算法 $KMAC$ 计算消息认证码

$$MAC_B=KMAC\left(WK_{BA},(T_B,R_B,T_A,R_A,N_B,N_A)\right) \quad (3)$$

然后卫星节点B将 T_B,R_B,N_B,MAC_B 发给卫星节点A。

第三步：卫星节点A收到消息后，将收到的消息存储下来，然后

① 利用哈希函数 H 计算主密钥 $MK_{AB}=\left(r_A\left(R_B+H(T_B,R_B)D\right),q_AQ_B\right)$；

② 利用密钥导出函数 KDF 计算工作密钥 $WK_{AB}=KDF(MK_{AB})$；

③ 利用消息认证码算法 $KMAC$ 计算消息认证码

$$MAC_A=KMAC\left(WK_{AB},(T_A,R_A,T_B,R_B,N_A,N_B)\right) \quad (4)$$

然后卫星节点A验证

$$MAC'_B=KMAC\left(WK_{AB},(T_B,R_B,T_A,R_A,N_B,N_A)\right)=MAC_B \quad (5)$$

如果验证通过，则计算会话密钥

$$SK_{AB}=KDF(WK_{AB},N_A,N_B) \quad (6)$$

将 MAC_A 发给卫星节点B，同时将 (ID_A,ID_B,WK_{AB}) 存储在非易失存储器中。如果验证未通过，则协商失败。

第四步：卫星节点B收到 MAC_A 后，验证

$$MAC'_A=KMAC\left(WK_{BA},(T_A,R_A,T_B,R_B,N_A,N_B)\right)=MAC_A \quad (7)$$

如果验证通过，则计算会话密钥

$$SK_{BA}=KDF(WK_{BA},N_A,N_B) \quad (8)$$

同时将 (ID_A,ID_B,WK_{BA}) 存储在非易失存储器中。如果验证未通过，则协商失败。

2.5 正确性证明

在设置阶段，椭圆曲线的生成元是 G，地面控制中心的公钥是 D。在注册阶段，卫星节点 i 通过与地面控制中心交互，得到私钥为 $pri\_key_i=(q_i,r_i)$，公钥为 $pub\_key_i=(Q_i,R_i)$。其中，卫星节点 i 的部分私钥是 q_i，部分公钥是 $Q_i=q_iG$，剩余部分私钥是 r_i，剩余部分公钥是 R_i，满足 $r_i\cdot G=R_i+h_i\cdot D$。

在认证和密钥协商阶段，卫星节点A计算的主密钥 MK_{AB} 满足 $MK_{AB}=(r_A(R_B+H(T_B,R_B)D),q_AQ_B)=(r_A(R_B+h_BD),q_AQ_B)=(r_Ar_BG,q_Aq_BG)$。

卫星节点B计算的主密钥 $MK_{BA}=(r_B(R_A+H(T_A,R_A)D),q_BQ_A)$ 满足 $MK_{AB}=(r_A(R_A+h_AD),q_BQ_A)=(r_Br_AG,q_Bq_AG)$。

由于 $r_Ar_BG=r_Br_AG$，$q_Aq_BG=q_Bq_AG$，故有 $MK_{AB}=MK_{BA}$，从而卫星节点A、B计算出的工作密钥满足 $WK_{AB}=KDF(MK_{AB})=KDF(MK_{BA})=WK_{BA}$，卫星节点A、B计算出的会话密钥满足 $SK_{AB}=KDF(WK_{AB},N_A,N_B)=KDF(WK_{BA},N_A,N_B)=SK_{BA}$。

2.6 会话密钥更新

由前文可知，认证和密钥协商需要进行三次交互。按照协议的流程，通信双方依次生成主密钥、工作密钥、会话密钥。当会话密钥使用期限截止或者发生密钥泄露、攻击时，双方需重新执行协议，协商出新的会话密钥。此时，协议的流程可以得到简化。在第一次认证和密钥协商阶段，双方生成会话密钥 SK 后，都将工作密钥 WK 进行了存储。在通信双方不变的情况下，每次认证和密钥协商都会生成同样的工作密钥 WK。因此，从第二次认证和密钥协商开始，双方可以省去计算主密钥和工作密钥的步骤，直接从非易失存储器中读取双方先前生成好的工作密钥 WK，由此协议的效率将会得到显著提升。

3 安全性分析

3.1 抗中间人攻击

由于卫星节点 i 的身份 ID_i 和卫星节点的部分公钥 Q_i 是绑定的，而中间人无法得知卫星节点的部分私钥 q_i，因此中间人将会生成错误的消息认证码 MAC，从而协商失败。因此，协议能够抵抗中间人攻击。

3.2 抗重放攻击

对于不同的会话密钥协商，协议都使用了不同的随机数 N_i，因此双方身份的有效性和会话密钥的新鲜性得到了保证。如果攻击者重放之前的会话密钥协商消息，那么双方将会计算出错误的消息认证码 MAC，从而协商失败。

3.3 前向/后向安全性

每次协商得到的会话密钥 SK 都和以往的不同，它的生成基于工作密钥 WK 和新鲜的随机数 N_i。即

使攻击者得到了这次会话的会话密钥，由于哈希函数的单向性，他也无法计算出双方的主密钥MK和工作密钥WK。因此，协议具有前向/后向安全性。

3.4　抗秘密信息泄露攻击

假设地面控制中心存储的卫星节点i的剩余部分私钥r_i信息泄露。由于卫星节点i使用的完整的公私钥对包含了两部分，一部分是自己产生的部分公私钥对(Q_i, q_i)，另一部分是地面控制中心产生的剩余部分公私钥对(R_i, r_i)。所以即使剩余部分私钥信息泄露，攻击者仍然无法计算出正确的工作密钥WK，从而消息认证失败。

4　计算分析和存储需求

在设置阶段，地面控制中心为每个卫星节点都配备了系统的公开参数，此阶段可离线完成。每个卫星节点需要存储椭圆曲线$E_p(a,b)$、生成元G、G的阶n、哈希函数H、消息认证码算法$KMAC$、密钥导出函数KDF、地面控制中心的公钥D。

在注册阶段，每个卫星节点和地面控制中心进行2次交互，共同生成该节点的公私钥对。地面控制中心需要完成2次点乘、1次点加和1次哈希操作。卫星节点需要完成2次点乘、1次点加和1次哈希操作。卫星节点需要存储自己完整的公私钥对。

在认证和密钥协商阶段，两个卫星节点A和B使用设置阶段中预存的公开参数，以及双方在注册阶段中生成的公私钥对，通过3次交互，生成双方共有的会话密钥。如果双方是第一次认证和密钥协商，卫星节点需要完成3次点乘、1次点加、1次哈希操作、2次$KMAC$和2次KDF操作；如果双方不是第一次认证和密钥协商，卫星节点只需完成2次$KMAC$和1次KDF操作。卫星节点需要存储对方的身份标识，对方的公钥、对方的随机数和双方共同的工作密钥WK。

表1总结了本方案与其它空间信息网络公钥管理方案的关键流程效率对比。表中各个运算的次数均为单个卫星节点所需计算的最大次数。由于$KMAC$和KDF都是基于哈希函数的运算，因此表中将它们视作哈希函数。

表1　与其它公钥管理方案的关键流程效率对比

Table 1　Efficiency comparison of key steps with other public-key management schemes

方案	方案一[17] (认证和密钥协商)	方案二[18] (认证和密钥协商)	方案三[19] (认证和密钥协商)	本方案（注册）	本方案（认证和密钥协商）	本方案（密钥更新）
交互次数	3	6	3	2	3	3
点乘次数	4	3	0	2	3	0
点加次数	2	0	0	1	1	0
哈希次数	3	6	3	1	5	3
对称加解密次数	0	1	1	0	0	0
矩阵乘法次数	0	0	3	0	0	0

在文献[19]中，作者经过实验得出，完成一次点乘运算大约需要1 000 μs，完成一次点加运算大约需要2.53 μs，完成一次哈希函数相关运算大约需要的时间是2.39 μs，完成一次对称算法加解密大约需要2.26 μs，完成一次矩阵乘法运算大约需要1 010 μs。当本文和其他方案采用同一套硬件时，在时间方面，本方案与已有方案的关键流程比较如表2和图4所示。

表2　与其它公钥管理方案的关键流程时间对比

Table 2　Time cost comparison of key steps with other public-key management schemes

方案	方案一[17] (认证和密钥协商)	方案二[18] (认证和密钥协商)	方案三[19] (认证和密钥协商)	本方案（注册）	本方案（认证和密钥协商）	本方案（密钥更新）
时间/μs	4 012.23	3 016.6	3 039.43	2 004.92	3 014.48	7.17

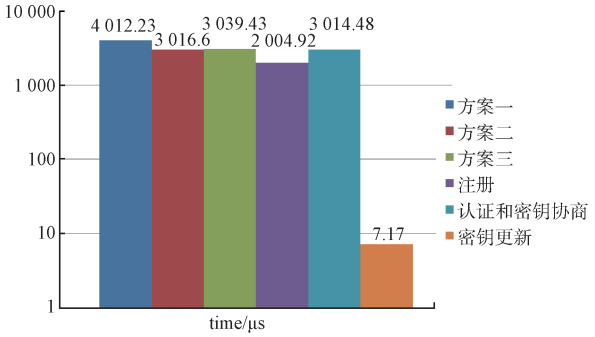

图 4 与其它公钥管理方案的关键流程时间对比

Fig. 4 Time cost comparison of key steps with other public-key management schemes

5 本方案的优势和不足

在传统的对称管理方案中，卫星节点需要存储和其余所有卫星节点的会话密钥，且存储的与每个卫星之间的会话密钥一般有很多组，这样就会造成很大的存储开销。采用本方案后，卫星节点只需存储当前的会话密钥，不用存储和其余每个卫星节点的会话密钥，有需要时进行会话密钥协商、存储即可，存储要求大幅减少。

采用本方案后，地面控制中心的计算负担也可以得到减轻。传统的对称管理方案需要适时对每个卫星节点执行更新密钥的操作，计算量大。采用公钥管理方案后，地面控制中心不必为每个卫星节点考虑更新密钥的操作，计算负担得以减轻，卫星节点间的生成/更新会话密钥只需由卫星双方进行协商得到。

另外，从安全性角度考虑，采用本方案可以具有更高的前向/后向安全性。在传统的对称管理方案中，卫星之间的会话密钥会使用一段时间，如果会话密钥泄露，那么不能保证前向/后向安全性。而在本方案中，每次会话的会话密钥都可以不同，这样就具有更高的前向/后向安全性。

本方案的不足之处主要在于认证和密钥协商阶段的效率较对称密码管理方案同阶段的要低，尤其是实现椭圆曲线上点的乘法操作需要消耗更多的计算资源，因此实时性不是特别高。

6 结束语

为保障空间信息网络信息传输的安全性，本文提出了一种基于椭圆曲线密码系统的公钥管理方案，为卫星节点提供入网认证、密钥协商和密钥更新等功能，实现了可认证、抗重放和前向/后向安全性等多种安全目标。对于卫星间的认证和密钥协商，本方案仅需 3 次交互即可完成。通过对方案进行安全性和效率分析，证实了本方案在空间信息网络中的实际可用性和效率上的优越性。

参考文献

[1] 闵士权 . 天基综合信息网探讨[J]. 国际太空, 2013(8): 46-54.

[2] 吴巍, 秦鹏, 冯旭, 等 . 关于天地一体化信息网络发展建设的思考[J]. 电信科学, 2017, 33(12): 3-9.
WU Wei, QIN Peng, FENG Xu, et al. Reflections on the development and construction of space-ground integration information network[J]. Telecommunications Science, 2017, 33(12): 3-9.

[3] KOHL J, NEUMAN C. The Kerberos Network Authentication Service(V5), RFC 1510, 1993. [EB/OL]. (1993-09-01) [2020-07-29]. http://www.ietf.org/rfc/rfc1510.txt.

[4] 林东岱, 曹天杰 . 应用密码学[M]. 北京: 科学出版社, 2009.

[5] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems [J]. Communications of the ACM, 1978, 21(2): 120-126.

[6] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE transactions on information theory, 1985, 31(4): 469-472.

[7] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 48(177):203-209.

[8] MILLER V S. Use of elliptic curves in cryptography[C]// Conference on The Theory and Application of Cryptographic Techniques. Berlin, Heidelberg: Springer, 1985: 417-426.

[9] LE A V, MATYAS S M, JOHNSON D B, et al. A public key extension to the common cryptographic architecture [J]. IBM System Journal, 1993, 32(3): 461-485.

[10] CRUICKSHANK H S. A security system for satellite networks[C]//Proceedings of Fifth International Conference on Satellite Systems for Mobile Communications and Navigation. Piscataway: IEEE Press, 1996: 187-190.

[11] 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.

[12] CHEN T H, LEE W B, CHEN H B. A self-verification authentication mechanism for mobile satellite communication systems[J]. Computers and Electrical Enginee-

ring, 2009, 35(1): 41-48.

[13] CHANG C C, CHENG T F, WU H L. An authentication and key agreement protocol for satellite communications [J]. International Journal of Communication Systems, 2014, 27(10): 1994–2006.

[14] ZHANG Y, CHEN J, HUANG B. An improved authentication scheme for mobile satellite communication systems[J]. International Journal of Satellite Communications and Networking, 2015, 33(2): 135-146.

[15] YAN L, CHANG Y, ZHANG S. Comments on 'an improved authentication scheme for mobile satellite communication systems'[J]. International Journal of Electronic Security and Digital Forensics, 2017, 9(4): 396-406.

[16] IBRAHIM M H, KUMARI S, DAS A K, et al. Jamming resistant non-interactive anonymous and unlinkable authentication scheme for mobile satellite networks[J]. Security and Communication Networks, 2016, 9(18): 5563-5580.

[17] MENG W, XUE K, XU J, et al. Low-latency authentication against satellite compromising for space information network[C]//2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS). IEEE, 2018: 237-244.

[18] QI M, CHEN J, CHEN Y. A secure authentication with key agreement scheme using ECC for satellite communication systems[J]. International Journal of Satellite Communications and Networking, 2019, 37(3): 234-244.

[19] MA R, CAO J, FENG D, et al. LAA: lattice-based access authentication scheme for IoT in space information networks[J]. IEEE Internet of Things Journal, 2020, 7(4): 2791-2805.

[作者简介]

杨静春　1993年生，博士，工程师。

陈韬鸣　1970年生，博士，副研究员。

蒋　鑫　1984年生，博士，研究员。

徐松艳　1978年生，硕士，研究员。

张道法　1964年生，硕士，研究员。

(本文编辑：潘三英)

(英文编辑：赵尹默)