面向无人机网络的属性代理签名方案

贺蕾[1,2]，马建峰[3,4]，魏大卫[1]

（1. 西安电子科技大学计算机科学与技术学院，陕西 西安 710071；2. 郑州轻工业大学计算机与通信工程学院，河南 郑州 450002；
3. 西安电子科技大学网络与信息安全学院，陕西 西安 710071；4. 西安电子科技大学陕西省网络与系统安全重点实验室， 陕西 西安 710071）

摘 要：为保护无人机网络中指挥机构发送给无人机的命令的完整性和认证性，需要使用数字签名对命令消息进行保护，该签名方案应保证无人机能及时收到签名，并且保护签名者的隐私。因此，提出了面向无人机网络的属性代理签名方案，并对其安全性进行了分析。所提方案在选择属性和选择消息攻击下具有存在的不可伪造性，而且能保护签名者的隐私。从计算开销和通信开销两方面对签名方案的效率进行了分析，并与其他相关签名方案进行了对比。结果表明，所提方案与其他方案在通信开销处于同一水平时具有更小的计算开销。

关键词：属性签名；代理签名；数字签名；无人机网络

中图分类号：TP309

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021210

Attribute-based proxy signature scheme for unmanned aerial vehicle networks

HE Lei[1,2], MA Jianfeng[3,4], WEI Dawei[1]

1. School of Computer Science and Technology, Xidian University, Xi'an 710071, China
2. College of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China
3. School of Cyber Engineering, Xidian University, Xi'an 710071, China
4. Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an 710071, China

Abstract: It is necessary to use digital signature scheme to protect integrity and authentication of commands sent by command agencies to unmanned aerial vehicle (UAV) in the UAV networks. Moreover, the signature scheme should ensure UAV can receive signature in time and protect privacy of signers. Therefore, an attribute-based proxy signature scheme for UAV networks was proposed and its security was analyzed. The proposed signature scheme has existential unforgeability under selective-attribute and chosen message attacks, and privacy of signers is protected. Its efficiency was analyzed in terms of computation costs and communication costs, and compared with other related signature schemes. The results indicate the proposed signature scheme has less computation costs when its communication costs are at the same level with other signature schemes.

Keywords: attribute-based signature, proxy signature, digital signature, unmanned aerial vehicle network

1 引言

近年来，无人机（UAV, unmanned aerial vehicle）得到了广泛的应用。无人机与指挥中心、地面控制站、卫星等共同构成了无人机网络，也称为无人机指挥控制与通信网络。无人机网络以无人机应用为核心，具有高机动性、动态拓扑、间断的通信连接、有限的电力供应和不断变化的链路质量等特点[1]。

收稿日期：2021−04−16；**修回日期**：2021−07−06

基金项目：促进海峡两岸科技合作联合基金资助项目（No.U1405255）；陕西省科技统筹创新工程计划项目（No.2016TZC-G-6-3）；中央高校基本科研业务费专项资金资助项目（No.SA-ZD161504）

Foundation Items: The Key Program of NSFC Grant (No.U1405255), The Shaanxi Science & Technology Coordination & Innovation Project (No.2016TZC-G-6-3), The Fundamental Research Funds for the Central Universities (No.SA-ZD161504)

无人机网络包括指挥中心、地面控制站、卫星和无人机等，如图 1 所示。每架无人机隶属于一个指挥中心，且该指挥中心拥有对该无人机的最高指挥权限。当指挥中心无法与无人机进行通信时，可以通过其他指挥机构，如地面控制站、卫星等，与无人机进行通信。

无人机执行任务时，必须保证所收到命令的完整性和认证性，即保证该命令是由指挥中心或经过授权的指挥机构发出的，而且没有被篡改。通常采用数字签名来保护命令的完整性和认证性。指挥中心发送命令及其签名给无人机，无人机在对签名进行验证后，根据验证结果决定是否执行该命令。

无人机在执行远程任务时远离指挥中心，可能无法及时收到指挥中心发来的命令，甚至无法收到命令。在这种情况下，指挥中心可以使用代理签名，临时授权距离无人机较近的指挥机构（如地面控制站）对无人机进行指挥，发送命令及其签名。而在一些应用中，指挥机构想要匿名地向无人机发送命令及签名，该签名并不包含与指挥机构身份有关的信息，可以通过使用基于属性的签名（ABS, attribute-based signature）实现。

本文主要研究工作如下。

1) 定义了属性代理签名及其安全模型。

2) 提出了用于无人机网络的属性代理签名（ABPS, attribute-based proxy signature）方案。

3) 对所提签名方案进行了安全性证明，结果表明，该方案具有选择属性和选择消息攻击下存在的不可伪造性（EUF-sA-CMA, existential unforgeability under selective-attribute and chosen message attacks），并且能保护签名者的隐私。

4) 从计算开销和通信开销两方面对所提方案的效率进行了分析，并与其他相关签名方案进行了对比。结果表明，所提方案具有更少的计算开销，而其通信开销与其他方案在同一水平。

2 相关工作

Maji 等[2]定义了 ABS 的安全性，构建了 ABS 的框架，并提出了 ABS 的具体实现。在 ABS 中，签名者使用属性集和相应的密钥对消息进行签名，验证者可以对签名进行验证，只有当属性集满足访问结构时，才能验证成功。Li 和 Kim[3]定义了隐藏的 ABS 及其安全模型，并提出了 2 种基于计算 Diffie-Hellman（CDH, computational Diffie-Hellman）困难问题的签名方案。Li 等[4]提出了 2 种支持门限访问结构的 ABS 方案，莫若等[5]提出了支持树形访问结构的可净化 ABS 方案，Gu 等[6]提出了支持单调访问结构的 ABS 方案。

在一些应用中，需要由多个属性权威对属性进行管理，为用户生成密钥。莫若等[7]提出了支持树形访问结构的多权威 ABS 方案。Guo 等[8]也提出了多权威 ABS 方案。Yang 等[9]提出了具有多个属性权威的顺序聚合 ABS 方案，在该签名方案中，不同的签名者可以对同一个消息进行签名，再将签名依次进行聚合。

为降低用户使用 ABS 计算签名的开销，Chen 等[10]提出了 2 个外包 ABS 方案，并证明了这 2 个

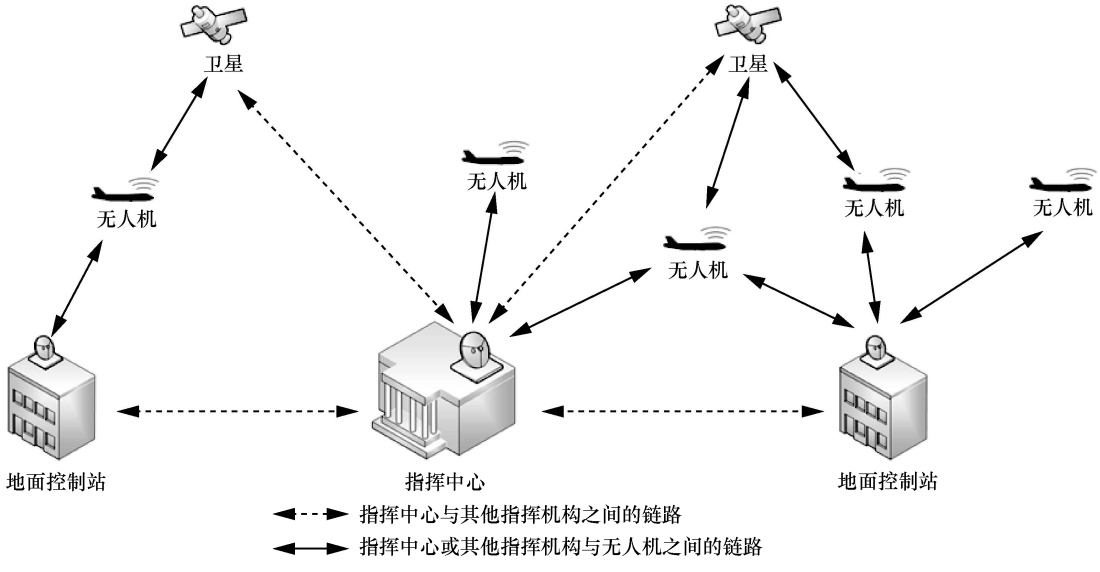


图 1 无人机网络

方案的安全性，通过将大量的签名计算外包给签名云服务提供者，降低了签名者的计算开销。Mo 等[11]提出了基于线性秘密共享的外包 ABS 方案，降低了签名者的计算开销，并证明了该方案的安全性。

为了降低计算签名和验证签名的计算开销，Cui 等[12]提出了可撤销的服务器辅助的 ABS 方案。在该签名方案中，服务器辅助完成签名生成和验证，以达到降低签名者和验证者计算开销的目的。而且，该签名方案还可以使被撤销的用户无法计算出签名。Xiong 等[13]也提出了服务器辅助的 ABS 方案，降低了签名者和验证者的计算开销，实现了基于线性秘密共享的访问结构，并能抵御合谋攻击。张应辉等[14]提出了一种服务器辅助且可验证的 ABS 方案。该方案同样降低了签名者和验证者的计算开销，能抵御合谋攻击，并且对服务器产生的部分签名进行了验证。Bao 等[15]提出了一种能抵御密钥泄露的服务器辅助的 ABS 方案，该签名方案需要对密钥进行更新。

Mambo 等[16]提出了代理签名。在代理签名中，通常包含 3 个参与者，分别是原始签名者（OS, original signer）、代理签名者（PS, proxy signer）和验证者。原始签名者授权代理签名者代替自己计算代理签名，验证者对该代理签名进行验证。Huang 等[17]提出了不需要随机预言机的代理签名方案，并对其安全性进行了证明。Wu 等[18]提出了基于身份的代理签名方案，并对其安全性进行了证明。Liu 等[19]定义了 ABPS 及其安全模型，提出了具体的 ABPS 方案，并对方案的安全性进行了证明。Sun 等[20]也提出了 ABPS 方案，并分析了方案的安全性。

3　预备知识

3.1　双线性对

设 G 和 G_T 是阶为素数 q 的循环群，G 的生成元为 g，若该映射满足下列要求，则映射 $e:G\times G\to G_T$ 为双线性映射。

1) 双线性：对于任意的 $g_1,g_2\in G$ 和 $a,b\in Z_q$，有 $e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$。

2) 非退化性：存在 $g_1,g_2\in G$，使 $e(g_1,g_2)\neq 1$。

3) 可计算性：对于任意的 $g_1,g_2\in G$，存在有效的算法能够计算出 $e(g_1,g_2)$。

3.2　CDH 困难问题假设

对于未知的 $x,y\in Z_q$，给定 $g,g^x,g^y\in G$，要求计算出 g^{xy}。

3.3　拉格朗日插值定理

设 $t(1)$, $t(2)$, …, $t(d)$是(d−1)次多项式 $t(\cdot)$上的 d 个点，S 是包含 d 个元素的集合，q 为素数。对于任何 $x\in Z_q$，可以通过拉格朗日插值定理求出 $t(x)=\sum_{i=1}^{d}t(i)\Delta_{i,S}(x)$。其中，拉格朗日系数定义为 $\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$。

4　系统模型

4.1　算法模型

ABPS 方案中主要包括属性权威、原始签名者、代理签名者和验证者。ABPS 方案主要由下列算法构成。

1) Setup。该算法输入为系统安全参数，输出公共参数 params 和主密钥 α。

2) Extract。该算法由属性权威运行，输入为公共参数 params、主密钥 α 和用户属性集合 ω，输出为用户的密钥。在 ABPS 方案中，属性权威依据原始签名者属性集合 ω_{OS} 和代理签名者属性集合 ω_{PS}，分别为它们生成密钥 sk_{OS} 和 sk_{PS}。

3) DelGen。该算法由原始签名者运行，用于为代理签名者生成授权。输入为 params、原始签名者生成的委托书 w、ω'_{OS} 和 sk_{OS}，且 $\omega'_{OS}\subseteq\omega_{OS}$；输出为原始签名者为代理签名者生成的授权 del。

4) DelVer。该算法由代理签名者运行，用于验证原始签名者生成的授权 del 是否有效，输入为 params、w、ω'_{OS} 和 del，输出为验证结果。若该授权是有效的，代理签名者可以基于 w 和 del 计算代理签名；否则，代理签名者不能基于 w 和 del 计算代理签名。

5) Sign。该算法由代理签名者运行，用于计算代理签名。输入为 params、w、del、ω'_{PS}、sk_{PS} 和消息 m，且 $\omega'_{PS}\subseteq\omega_{PS}$；输出为计算出的代理签名 σ。

6) Verify。该算法由验证者运行，用于验证代理签名是否有效。其输入为 params、w、ω'_{PS}、m 和 σ，输出为布尔类型的验证结果。若该代理签名是有效的，则输出 Accept；否则，输出 Reject。

4.2　安全模型

ABPS 方案的安全性主要包括不可伪造性和签名者的隐私性。不可伪造性要求如下：若敌手没有属性集 ω 对应的密钥且 $\omega^*\subseteq\omega$，则不能计算出属性

集 ω^* 对应的签名。签名者的隐私性要求签名不泄露签名者的身份信息。

4.2.1 不可伪造性

根据文献[17-19]，ABPS 方案中的敌手可分为三类，分别为 A_I、A_{II} 和 A_{III}。A_I 只拥有原始签名者和代理签名者的公钥；A_{II} 和 A_{III} 除了拥有原始签名者和代理签名者的公钥以外，还分别拥有代理签名者的私钥 sk_{PS} 和原始签名者的私钥 sk_{OS}。若 ABPS 方案能抵御 A_{II} 和 A_{III} 的攻击，则其也能抵御 A_I 的攻击。因此，在安全模型中只考虑 A_{II} 和 A_{III} 的攻击。对于不可伪造性，主要研究 EUF-sA-CMA。

1) 能抵御 A_{II} 攻击的 EUF-sA-CMA

通过下面的游戏定义能抵御 A_{II} 攻击的 EUF-sA-CMA。

初始化阶段。选择要挑战的属性集 ω^*，且 $|\omega^*| \leqslant d$。其中，d 是预先定义的参数。

系统建立阶段。挑战者 C 运行 Setup 算法生成公共参数 params 和主密钥，运行 Extract 算法为原始签名者和代理签名者分别生成密钥对(pk_{OS}, sk_{OS})和(pk_{PS}, sk_{PS})。将 params、原始签名者公钥 pk_{OS}，以及代理签名者的公钥和私钥(pk_{PS}, sk_{PS})发送给 A_{II}。

查询阶段。A_{II} 可以向私钥生成预言机、授权生成预言机和签名预言机分别进行多项式次数的查询。

伪造阶段。A_{II} 输出关于消息 m^*、属性集 ω^* 和委托书 w^* 的签名 σ^*。

若该伪造满足以下条件，则认为 A_{II} 赢得了游戏。

① A_{II} 从未向私钥生成预言机查询过属性集 ω_{OS}，且 $\omega^* \subseteq \omega_{OS}$。

② A_{II} 从未向授权生成预言机查询过(w^*, ω^*)。

③ A_{II} 从未向签名预言机查询过(m^*, w^*, ω^*)。

④ 签名 σ^* 是关于消息 m^*、ω^* 和委托书 w^* 的有效签名。

定义 1 若敌手 A_{II} 在上面的游戏中获胜的概率是可忽略的，则称该 ABPS 方案具有能抵御 A_{II} 攻击的 EUF-sA-CMA。

2) 能抵御 A_{III} 攻击的 EUF-sA-CMA

通过下面的游戏定义能抵御 A_{III} 攻击的 EUF-sA-CMA。

初始化阶段。选择要挑战的属性集 ω^*，且 $|\omega^*| \leqslant d$。其中，d 是预先定义的参数。

系统建立阶段。挑战者 C 运行 Setup 算法生成公共参数 params 和主密钥，运行 Extract 算法为原始签名者和代理签名者分别生成密钥对(pk_{OS}, sk_{OS})和(pk_{PS}, sk_{PS})。将 params、代理签名者公钥 pk_{PS}，以及原始签名者的公钥和私钥(pk_{OS}, sk_{OS})发送给 A_{III}。

查询阶段。A_{III} 可以向私钥生成预言机和签名预言机分别进行多项式次数的查询。

伪造阶段。A_{III} 输出关于消息 m^*、属性集 ω^* 和委托书 w^* 的签名 σ^*。

若该伪造满足以下条件，则认为 A_{III} 赢得了游戏。

1) A_{III} 从未向私钥生成预言机查询过属性集 ω_{PS}，且 $\omega^* \subseteq \omega_{PS}$。

2) A_{III} 从未向签名预言机查询过(m^*, w^*, ω^*)。

3) 签名 σ^* 是关于消息 m^*、属性集 ω^* 和委托书 w^* 的有效签名。

定义 2 若敌手 A_{III} 在上面的游戏中获胜的概率是可忽略的，则称该 ABPS 方案具有能抵御 A_{III} 攻击的 EUF-sA-CMA。

4.2.2 签名者的隐私性

通过下面的游戏对签名者的隐私性进行定义。

系统建立阶段。挑战者 C 运行 Setup 算法生成公共参数 params 和主密钥，并将 params 和主密钥发送给敌手 A。

查询阶段。A 可以向私钥生成预言机查询属性集 ω_1^* 和 ω_2^*，并获取相应的私钥 $sk_{\omega_1^*}$ 和 $sk_{\omega_2^*}$。

挑战阶段。A 输出消息 m^* 和属性集 ω_1^*、ω_2^*、ω^*，且 $\omega^* \subseteq \omega_1^* \cap \omega_2^*$，$|\omega^*| \leqslant d$。挑战者 C 随机挑选 $u \in \{1,2\}$，使用 ω^* 和密钥 $sk_{\omega_u^*}$ 计算消息 m^* 的签名 σ^*，并将该签名发送给 A。

猜测阶段。A 猜测 σ^* 是由 ω_1^* 或 ω_2^* 计算得出的，并输出 $u' \in \{1,2\}$。若 A 猜测 σ^* 是由 ω_1^* 计算得出的，则输出 $u'=1$；否则，输出 $u'=2$。若 $u'=u$，则 A 赢得该游戏。

A 赢得上述游戏的优势被定义为 $|\Pr[u'=u]-0.5|$。

定义3 若不存在敌手 A 能以不可忽略的优势赢得上述游戏，则认为该 ABPS 方案保护了签名者的隐私。

5 面向无人机网络的 ABPS 方案描述

5.1 总体方案

在本文所提出的 ABPS 方案中，主要包括属性权威、指挥中心、地面控制站和无人机，如图 2 所

示。其中，指挥中心为原始签名者，地面控制站为代理签名者，无人机为验证者。指挥中心为地面控制站生成委托书和授权，地面控制站代表指挥中心计算代理签名，并发送给无人机进行验证。方案的总体流程如下。

1) 生成公共参数和主密钥。属性权威为指挥中心和地面控制站生成密钥。

2) 指挥中心生成委托书 w 和授权 del，并将它们发送给地面控制站。

3) 地面控制站验证收到的授权。若该授权是有效的，则可以计算代理签名；否则，不能计算代理签名。

4) 地面控制站依据收到的委托书和授权计算出消息 m 的代理签名。

5) 无人机收到签名后，对其进行验证，并输出验证结果。

5.2　算法描述

本文所提出的签名方案主要包括以下算法。

1) Setup

设 G 和 G_T 是阶为素数 q 的循环群，映射 $e:G\times G\to G_T$ 为双线性映射，选择随机生成元 $g\in G$，将属性定义为 Z_q 中的元素，定义默认属性集 $\Omega=\{\Omega_1,\Omega_2,\cdots,\Omega_{d-1}\}$。选择随机数 $\alpha\in Z_q^*$ 和随机元素 $g_2\in G$，哈希函数 $H_1,H_2,H_3:\{0,1\}^*\to G$，计算 $g_1=g^{\alpha}$ 和 $Z=e(g_1,g_2)$。公开参数 params 为 $(g,g_1,g_2,Z,d,H_1,H_2,H_3)$，主密钥为 α。

2) Extract

该算法分别为原始签名者和代理签名者生成密钥。设原始签名者和代理签名者的属性集分别为 ω_o 和 ω_p，生成属性集 $\hat{\omega}_o=\omega_o\cup\Omega$ 和 $\hat{\omega}_p=\omega_p\cup\Omega$，选择($d$−1)次多项式 $t(\cdot)$，且 $t(0)=\alpha$。生成随机数 $r_{i_{o,\hat{v}_o}}\in Z_q$，计算原始签名者的密钥 $D_{i_{o,\hat{v}_o}}=(d_{i_{o,\hat{v}_o}0},d_{i_{o,\hat{v}_o}1})=(g_2^{t(i_{o,\hat{v}_o})}H_1(i_{o,\hat{v}_o})^{r_{i_{o,\hat{v}_o}}},g^{r_{i_{o,\hat{v}_o}}})$，其中 $i_{o,\hat{v}_o}\in\hat{\omega}_o$，且$1\leqslant\hat{v}_o\leqslant|\hat{\omega}_o|$。类似地，生成随机数 $r_{i_{p,\hat{v}_p}}\in Z_q$，计算代理签名者的密钥 $D_{i_{p,\hat{v}_p}}=(d_{i_{p,\hat{v}_p}0},d_{i_{p,\hat{v}_p}1})=(g_2^{t(i_{p,\hat{v}_p})}H_1(i_{p,\hat{v}_p})^{r_{i_{p,\hat{v}_p}}},g^{r_{i_{p,\hat{v}_p}}})$，其中 $i_{p,\hat{v}_p}\in\hat{\omega}_p$，且$1\leqslant\hat{v}_p\leqslant|\hat{\omega}_p|$。

3) DelGen

原始签名者选择属性集 $\omega'_o=\{\omega_1,\omega_2,\cdots,\omega_{k_o}\}\subseteq\omega_o$ 和 $\Omega'_o=\{\Omega_{k_o+1},\Omega_{k_o+2},\cdots,\Omega_d\}\subseteq\Omega$，其中 $1\leqslant k_o\leqslant d$。设 $\hat{\omega}'_o=\omega'_o\cup\Omega'_o=\{i_{o,1},i_{o,2},\cdots,i_{o,v},\cdots,i_{o,d}\}$，选择($d$−1)次多项式 $t'_o(\cdot)$，且 $t'_o(0)=0$。选择随机数 $r'_{i_{o,v}},s_{i_{o,v}}\in Z_q$，其中 $i_{o,v}\in\hat{\omega}'_o$，$1\leqslant v\leqslant d$。原始签名者为代理签名者生成委托书 w，计算授权 del=$(\sigma_{i_o1},\sigma_{i_{o,v}2},\sigma_{i_{o,v}3})$。其中，$\sigma_{i_o1}=\prod_{v=1}^{d}(\sigma_{i_{o,v}1})^{\Delta_{i_{o,v},S_o}(0)}$，并且 $\sigma_{i_{o,v}1}=d_{i_{o,v}0}H_1(i_{o,v})^{r'_{i_{o,v}}}\ g_2^{t'_o(i_{o,v})}H_2(w)^{s_{i_{o,v}}}$，$\sigma_{i_{o,v}2}=d_{i_{o,v}1}g^{r'_{i_{o,v}}}$，$\sigma_{i_{o,v}3}=g^{s_{i_{o,v}}}$。原始签名者发送 $(w,\sigma_{i_o1},\sigma_{i_{o,v}2},\sigma_{i_{o,v}3})$ 给代理签名者。

4) DelVer

代理签名者收到原始签名者发来的委托书和授权后，通过下面的验证式对该授权进行验证。若该等式成立，则认为该授权是有效的；否则，认为该授权是无效的。

$$\frac{e(g,\sigma_{i_o1})}{\prod_{v=1}^{d}(e(H_1(i_{o,v}),\sigma_{i_{o,v}2})e(H_2(w),\sigma_{i_{o,v}3}))^{\Delta_{i_{o,v},S_o}(0)}}=Z$$

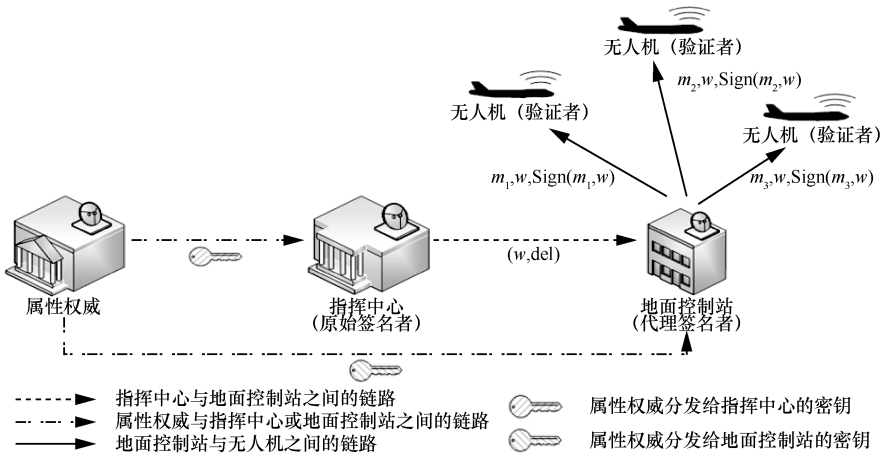


图 2　总体方案

5) Sign

代理签名者根据原始签名者的委托书和授权计算消息 m 的签名。代理签名者选择属性集 $\omega'_p = \{\omega_1, \omega_2, \cdots, \omega_{k_p}\} \subseteq \omega_p$ 和 $\Omega'_p = \{\Omega_{k_p+1}, \Omega_{k_p+2}, \cdots, \Omega_d\} \subseteq \Omega$，其中 $1 \leqslant k_p \leqslant d$。设 $\hat{\omega}'_p = \omega'_p \cup \Omega'_p = \{i_{p,1}, i_{p,2}, \cdots, i_{p,v}, \cdots, i_{p,d}\}$，选择 $(d-1)$ 次多项式 $t'_p(\cdot)$，且 $t'_p(0) = 0$。选择随机数 $r'_{i_{p,v}}, s_{i_{p,v}} \in Z_q$，其中 $i_{p,v} \in \hat{\omega}'_p$，$1 \leqslant v \leqslant d$。代理签名者计算签名 $\sigma = (\sigma_{i_{p}1}, \sigma_{i_{p,v}2}, \sigma_{i_{p,v}3}, \sigma_{i_{p,v}4}, \sigma_{i_{p,v}5})$。其中 $\sigma_{i_p 1} = \sigma_{i_o 1} \prod_{v=1}^{d} (\sigma_{i_{p,v}1})^{\Delta_{i_{p,v},S_p}(0)}$，并且 $\sigma_{i_{p,v}1} = d_{i_{p,v}0} H_1(i_{p,v})^{r'_{i_{p,v}}} g_2^{t'_p(i_{p,v})} H_3(m)^{s_{i_{p,v}}}$，$\sigma_{i_{p,v}2} = d_{i_{p,v}1} g^{r'_{i_{p,v}}}$，$\sigma_{i_{p,v}3} = \sigma_{i_{o,v}2}$，$\sigma_{i_{p,v}4} = \sigma_{i_{o,v}3}$，$\sigma_{i_{p,v}5} = g^{s_{i_{p,v}}}$。

6) Verify

验证者收到代理签名者发来的数字签名后，通过下面的验证式对该签名进行验证。若该等式成立，则认为该签名是有效的，输出布尔值 Accept；否则，认为该签名是无效的，输出布尔值 Reject。

$$\frac{e(g,\sigma_{i_p 1})}{\prod_{v=1}^{d}(e(H_1(i_{p,v}),\sigma_{i_{p,v}2})e(H_3(m),\sigma_{i_{p,v}5}))^{\Delta_{i_{p,v},S_p}(0)}} \cdot \frac{1}{\prod_{v=1}^{d}(e(H_1(i_{o,v}),\sigma_{i_{p,v}3})e(H_2(w),\sigma_{i_{p,v}4}))^{\Delta_{i_{o,v},S_o}(0)}} = Z^2$$

6 方案分析

6.1 正确性分析

定理 1 本文所提出的 ABPS 方案具有正确性。

证明 分两步对方案的正确性进行分析。首先分析 DelGen 和 DelVer 算法的正确性，然后分析 Sign 和 Verify 算法的正确性。

1) DelGen 和 DelVer 算法的正确性

$$\frac{e(g,\sigma_{i_o 1})}{\prod_{v=1}^{d}(e(H_1(i_{o,v}),\sigma_{i_{o,v}2})e(H_2(w),\sigma_{i_{o,v}3}))^{\Delta_{i_{o,v},S_o}(0)}} = \prod_{v=1}^{d}\left(\frac{e(g,d_{i_{o,v}0}H_1(i_{o,v})^{r'_{i_{o,v}}} g_2^{t'_o(i_{o,v})} H_2(w)^{s_{i_{o,v}}})}{e(H_1(i_{o,v}),d_{i_{o,v}1}g^{r'_{i_{o,v}}})e(H_2(w),g^{s_{i_{o,v}}})}\right)^{\Delta_{i_{o,v},S_o}(0)} = \prod_{v=1}^{d} e(g, g_2^{t_o(i_{o,v})} g_2^{t'_o(i_{o,v})})^{\Delta_{i_{o,v},S_o}(0)} = e(g,g_2^{\alpha}) = Z$$

2) Sign 和 Verify 算法的正确性

$$\frac{e(g,\sigma_{i_p 1})}{\prod_{v=1}^{d}(e(H_1(i_{p,v}),\sigma_{i_{p,v}2})e(H_3(m),\sigma_{i_{p,v}5}))^{\Delta_{i_{p,v},S_p}(0)}} \cdot \frac{1}{\prod_{v=1}^{d}(e(H_1(i_{o,v}),\sigma_{i_{p,v}3})e(H_2(w),\sigma_{i_{p,v}4}))^{\Delta_{i_{o,v},S_o}(0)}} = \prod_{v=1}^{d}\left(\frac{e(g,d_{i_{p,v}0}H_1(i_{p,v})^{r'_{i_{p,v}}} g_2^{t'_p(i_{p,v})} H_3(m)^{s_{i_{p,v}}})}{e(H_1(i_{p,v}),d_{i_{p,v}1}g^{r'_{i_{p,v}}})e(H_3(m),g^{s_{i_{p,v}}})}\right)^{\Delta_{i_{p,v},S_p}(0)} \cdot \frac{e(g,\sigma_{i_o 1})}{\prod_{v=1}^{d}(e(H_1(i_{o,v}),\sigma_{i_{o,v}2})e(H_2(w),\sigma_{i_{o,v}3}))^{\Delta_{i_{o,v},S_o}(0)}} = ZZ = Z^2$$

定理 1 证毕。

6.2 不可伪造性

对于不可伪造性，分别证明所提签名方案具有能抵御 A_{II} 攻击的 EUF-sA-CMA 和能抵御 A_{III} 攻击的 EUF-sA-CMA，然后得出结论，所提签名方案具有 EUF-sA-CMA。

定理 2 若 CDH 问题是困难的，则所提 ABPS 方案具有能抵御 A_{II} 攻击的 EUF-sA-CMA。

证明 假设敌手 A_{II} 能以优势 ε 攻击所提 ABPS 方案。在此基础上，构建算法 B 能以优势 ε' 攻击 CDH 问题。A_{II} 向随机预言机（H_1-oracle, H_2-oracle, H_3-oracle）、私钥生成预言机、授权生成预言机和签名预言机分别进行 $q_{H_1}, q_{H_2}, q_{H_3}, q_K, q_D, q_S$ 次查询。给定 CDH 问题的随机实例 $(g, X = g^x, Y = g^y)$，其中，$x, y \in Z_q$，使用算法 B 计算 g^{xy}。

设默认属性集为 $\Omega = \{\Omega_1, \Omega_2, \cdots, \Omega_{d-1}\}$，其中 d 为预先定义的整数。A_{II} 输出挑战的属性集 ω^*，且 $|\omega^*| = k$，$k \leqslant d$。B 随机选择 $\zeta \in \{1,2,\cdots,q_{H_2}\}$，$\delta \in \{1,2,\cdots,q_{H_3}\}$，以及子集 $\Omega^* \subseteq \Omega$ 且 $|\Omega^*| = d - k$。设 $g_1 = X$，$g_2 = Y$。

H_1-oracle: B 维护列表 H_1-list。当 A_{II} 向 H_1-oracle 查询 i 时，B 在 H_1-list 中进行搜索。若该列表中存在 i，则输出相应的 $H_1(i)$。否则，若 $i \in \omega^* \cup \Omega^*$，则 $H_1(i) = g^{b_i}$；若 $i \notin \omega^* \cup \Omega^*$，则 $H_1(i) = g_1^{-b_i} g^{a_i}$。其中，$a_i$ 和 b_i 是随机数，且 $a_i, b_i \in Z_q$。B 输出计算出的 $H_1(i)$，并将 $(i, H_1(i))$ 添加到 H_1-list 中。

H_2-oracle: B 维护列表 H_2-list。当 A_{II} 向

H_2-oracle 查询$w_{i'}$时，B 在H_2-list 中进行搜索。若该列表中存在$w_{i'}$，则输出相应的$H_2(w_{i'})$。否则，若 $i'\neq\zeta$，则 $H_2(w_{i'})=g_1^{c'_{i'}}g^{a'_{i'}}$；若 $i'=\zeta$，则 $H_2(w_{i'})=g^{a'_{i'}}$。其中，$a'_{i'}$和$c'_{i'}$是随机数，且$a'_{i'},c'_{i'}\in Z_q$。B 输出计算得到的$H_2(w_{i'})$，并将$(w_{i'},H_2(w_{i'}))$添加到H_2-list 中。

H_3-oracle: B 维护列表H_3-list。当 A_{II} 向H_3-oracle 查询$m_{i''}$时，B 在H_3-list 中进行搜索。若该列表中存在$m_{i''}$，则输出相应的$H_3(m_{i''})$。否则，若 $i''\neq\delta$，则 $H_3(m_{i''})=g_1^{c''_{i''}}g^{a''_{i''}}$；若 $i''=\delta$，则 $H_3(m_{i''})=g^{a''_{i''}}$。其中，$a''_{i''}$和$c''_{i''}$是随机数，且$a''_{i''},c''_{i''}\in Z_q$。B 输出计算出的$H_3(m_{i''})$，并将$(m_{i''},H_3(m_{i''}))$添加到$H_3$-list 中。

私钥生成预言机：A_{II}可以向私钥生成预言机查询属性集ω，且ω^*不是ω的子集。设集合$\Gamma=(\omega\cap\omega^*)\cup\Omega^*$，$\Gamma\subseteq\Gamma'\subseteq S$，$|\Gamma'|=d-1$，$S=\Gamma'\cup\{0\}$。

对于$i\in\Gamma'$，输出密钥$(g_2^{f_i}H_1(i)^{r_i},g^{r_i})$，其中$f_i$和$r_i$是随机数，且$f_i,r_i\in Z_q$。

对于 $i\notin\Gamma'$，设 $r_i=\dfrac{\Delta_{0,S}(i)}{b_i}y+r'_i$，$t(i)=\sum_{j\in\Gamma'}\Delta_{j,S}(i)t(j)+\Delta_{0,S}(i)t(0)$，其中 t(0)=x，$r_i,r'_i\in Z_q$。输出密钥为$(g_2^{\frac{a_i\Delta_{0,S}(i)}{b_i}+\sum_{j\in\Gamma'}\Delta_{j,S}(i)t(j)}H_1(i)^{r'_i},g_2^{\frac{\Delta_{0,S}(i)}{b_i}}g^{r'_i})$。

授权生成预言机：A_{II}可以向授权生成预言机查询委托书w和属性集ω。

若ω^*不是ω的子集，B 可以获取私钥生成预言机生成的密钥，进而计算出授权。

若$\omega^*\subseteq\omega$，且$H_2(w_{i'})=g^{a'_{i'}}$，游戏终止。

若$\omega^*\subseteq\omega$，且$H_2(w_{i'})\neq g^{a'_{i'}}$，B 从$\Omega$中选择含有$(d-|\omega|)$个元素的子集$\Omega'$，设$\omega\cup\Omega'=\{i_{o,1},i_{o,2},\cdots,i_{o,v},\cdots,i_{o,d}\}$。对于$1\leqslant v\leqslant(d-1)$，B 选择随机数$\tau_{o,v},r_{i_{o,v}},s_{o,v}\in Z_q$，设$t_o(i_{o,v})=\tau_{o,v}$，计算$\sigma_{i_{o,v}1}=g_2^{t_o(i_{o,v})}H_1(i_{o,v})^{r_{i_{o,v}}}H_2(w)^{s_{o,v}}$，$\sigma_{i_{o,v}2}=g^{r_{i_{o,v}}}$，$\sigma_{i_{o,v}3}=g^{s_{o,v}}$。对于 $v=d$，B 选择随机数$r_{i_{o,d}},s'_{o,d}\in Z_q$，设$s_{o,d}=-\dfrac{\Delta_{0,S_o}(i_{o,d})}{c'_{i_{o,d}}}y+s'_{o,d}$，计算$\sigma_{i_{o,d}1}=g_2^{\sum_{v=1}^{d-1}\Delta_{i_{o,v},S_o}(i_{o,d})t_o(i_{o,v})}g_2^{-\frac{\Delta_{0,S_o}(i_{o,d})}{c'_{i_{o,d}}}a'_{i_{o,d}}}H_1(i_{o,d})^{r_{i_{o,d}}}g_1^{c'_{i_{o,d}}s'_{o,d}}\cdot g^{a'_{i_{o,d}}s'_{o,d}}$，$\sigma_{i_{o,d}2}=g^{r_{i_{o,d}}}$，$\sigma_{i_{o,d}3}=g_2^{-\frac{\Delta_{0,S_o}(i_{o,d})}{c'_{i_{o,d}}}}g^{s'_{o,d}}$。据此，B 可以计算出$\sigma_{i_{o}1}$，并返回相应的授权给 A_{II}。

签名预言机：A_{II}可以向签名预言机查询消息m关于委托书w和属性集ω的签名。

若$H_2(w_{i'})=g^{a'_{i'}}$，$H_3(m_{i''})=g^{a''_{i''}}$，游戏终止；否则，B 可以计算出授权和签名，并将签名返回给 A_{II}。

伪造：敌手 A_{II}生成对于消息m^*、属性集ω^*和Ω^{**}、委托书w^*的签名σ^*。若$H_2(w^*)\neq g^{a'_\zeta}$，或$H_3(m^*)\neq g^{a''_\delta}$，或$\Omega^{**}\neq\Omega^*$，游戏终止。否则，该伪造的签名可以通过验证，即该伪造的签名满足

$$\left(\frac{e(g,\sigma^*_{i_p1})}{\prod_{v=1}^{d}(e(H_1(i_{p,v}),\sigma^*_{i_{p,v}2})e(H_3(m),\sigma^*_{i_{p,v}5}))^{\Delta_{i_{p,v},S_p}(0)}}\cdot\frac{1}{\prod_{v=1}^{d}(e(H_1(i_{o,v}),\sigma^*_{i_{p,v}3})e(H_2(w),\sigma^*_{i_{p,v}4}))^{\Delta_{i_{o,v},S_o}(0)}}\right)^{\frac12}=$$

$$\left(\frac{e(g,\sigma^*_{i_p1})}{\prod_{v=1}^{d}(e(g^{b_{i_{p,v}}},\sigma^*_{i_{p,v}2})e(g^{a''_\delta},\sigma^*_{i_{p,v}5}))^{\Delta_{i_{p,v},S_p}(0)}}\cdot\frac{1}{\prod_{v=1}^{d}(e(g^{b_{i_{o,v}}},\sigma^*_{i_{p,v}3})e(g^{a'_\zeta},\sigma^*_{i_{p,v}4}))^{\Delta_{i_{o,v},S_o}(0)}}\right)^{\frac12}=$$

$$\left(\frac{e(g,\sigma^*_{i_p1})}{\prod_{v=1}^{d}(e(g,(\sigma^*_{i_{p,v}2})^{b_{i_{p,v}}})e(g,(\sigma^*_{i_{p,v}5})^{a''_\delta}))^{\Delta_{i_{p,v},S_p}(0)}}\cdot\frac{1}{\prod_{v=1}^{d}(e(g,(\sigma^*_{i_{p,v}3})^{b_{i_{o,v}}})e(g,(\sigma^*_{i_{p,v}4})^{a'_\zeta}))^{\Delta_{i_{o,v},S_o}(0)}}\right)^{\frac12}=$$

$e(g_1,g_2)=e(g,g^{xy})$

因此，B 可以计算g^{xy}为

$$g^{xy}=\left(\frac{\sigma^*_{i_p1}}{\prod_{v=1}^{d}((\sigma^*_{i_{p,v}2})^{b_{i_{p,v}}}(\sigma^*_{i_{p,v}5})^{a''_\delta})^{\Delta_{i_{p,v},S_p}(0)}}\cdot\frac{1}{\prod_{v=1}^{d}((\sigma^*_{i_{p,v}3})^{b_{i_{o,v}}}(\sigma^*_{i_{p,v}4})^{a'_\zeta})^{\Delta_{i_{o,v},S_o}(0)}}\right)^{\frac12}$$

至此，B 解决了给定的 CDH 问题实例，可计算出$\varepsilon'\approx\dfrac{\varepsilon}{q_{H_2}^2q_{H_3}\binom{d-k}{d-1}^2}$。因此，本文提出的 ABPS

方案具有能抵御 A_{II} 攻击的 EUF-sA-CMA。定理 2 证毕。

定理 3 若 CDH 问题是困难的，则本文提出的 ABPS 方案具有能抵御 A_{III} 攻击的 EUF-sA-CMA。

证明 该定理的证明过程与定理 2 的证明过程类似。敌手 A_{III} 可以对 H_1 -oracle、H_2 -oracle、H_3-oracle、私钥生成预言机和签名预言机进行多项式次数的查询，并伪造签名。B 解决给定的 CDH 问题实例的优势为 $\varepsilon' \approx \dfrac{\varepsilon}{q_{H_2} q_{H_3} \binom{d-k}{d-1}}$。因此，本文提出的 ABPS 方案具有能抵御 A_{III} 攻击的 EUF-sA-CMA。定理 3 证毕。

根据定理 2 和定理 3，可得本文提出的 ABPS 方案具有 EUF-sA-CMA。

6.3 签名者隐私

在所提方案中，原始签名者生成的授权可以看作对委托书的签名，而且，代理签名中包含有原始签名者生成的授权。因此，对签名者隐私的保护包含对原始签名者和代理签名者的隐私的保护。

定理 4 本文提出的 ABPS 方案保护了原始签名者的隐私。

证明 挑战者 C 选择安全参数，运行 Setup 算法生成公开参数 params 和主密钥 α，并将(params, α)发送给敌手 A。A 输出属性集 $\omega^*_{u,o}$，设 $\hat{\omega}^*_{u,o} = \omega^*_{u,o} \cup \Omega$，其中 $u \in \{1,2\}$。选择随机数 $r_{u,i_{o,\hat{v}}} \in Z_q$，并计算密钥 $\mathrm{sk}_{\hat{\omega}^*_{u,o}} = (d_{u,i_{o,\hat{v}}0}, d_{u,i_{o,\hat{v}}1})$。其中，$d_{u,i_{o,\hat{v}}0} = g_2^{t_{u,o}(i_{o,\hat{v}})} H_1(i_{o,\hat{v}})^{r_{u,i_{o,\hat{v}}}}$，$d_{u,i_{o,\hat{v}}1} = g^{r_{u,i_{o,\hat{v}}}}$，$t_{u,o}(\cdot)$ 是(d−1) 次多项式且 $t_{u,o}(0) = \alpha$，$i_{o,\hat{v}} \in \hat{\omega}^*_{u,o}$，$1 \leqslant \hat{v} \leqslant |\hat{\omega}^*_{u,o}|$，$u \in \{1,2\}$。

敌手 A 选择委托书 w^* 和属性集 ω^*_o，且 $\omega^*_o \subseteq \omega^*_{1,o} \cap \omega^*_{2,o}$，$|\omega^*_o| = k_o \leqslant d$。挑战者 C 随机选择 $u \in \{1,2\}$，$\Omega'_o \subseteq \Omega$ 且 $|\Omega'_o| = d - k_o$，$r'_{i_{o,v}}, s_{i_{o,v}} \in Z_q$ 且 $i_{o,v} \in \omega^*_o \cup \Omega'_o$，$1 \leqslant v \leqslant d$。可以计算出授权 $(\sigma^*_{u,i_{o,v}1}, \sigma^*_{u,i_{o,v}2}, \sigma^*_{u,i_{o,v}3})$。其中，$\sigma^*_{u,i_{o,v}1} = \prod_{v=1}^{d} (\sigma^*_{u,i_{o,v}1})^{\Delta_{i_{o,v},S_o}(0)}$ 且 $\sigma^*_{u,i_{o,v}1} = d_{u,i_{o,v}0} H_1(i_{o,v})^{r'_{i_{o,v}}} g_2^{t'_o(i_{o,v})} H_2(w^*)^{s_{i_{o,v}}}$，$\sigma^*_{u,i_{o,v}2} = d_{u,i_{o,v}1} g^{r'_{i_{o,v}}}$，$\sigma^*_{u,i_{o,v}3} = g^{s_{i_{o,v}}}$。$t'_o(\cdot)$ 是(d−1)次多项式且 $t'_o(0) = 0$。接下来，证明由密钥 $\mathrm{sk}_{\hat{\omega}^*_{1,o}}$ 生成的授权也可以由密钥 $\mathrm{sk}_{\hat{\omega}^*_{2,o}}$ 生成。

由密钥 $sk_{\hat{\omega}^*_{1,o}}$ 生成的授权 $\sigma^*_{1,i_{o}1}$ 中的 $\sigma^*_{1,i_{o,v}1}$ 和 $\sigma^*_{1,i_{o,v}2}$ 可以写成 $\sigma^*_{1,i_{o,v}1} = d_{2,i_{o,v}0} \dfrac{d_{1,i_{o,v}0}}{d_{2,i_{o,v}0}} H_1(i_{o,v})^{r'_{i_{o,v}}} \cdot g_2^{t'_o(i_{o,v})} H_2(w^*)^{s_{i_{o,v}}}$，$\sigma^*_{1,i_{o,v}2} = d_{2,i_{o,v}1} \dfrac{d_{1,i_{o,v}1}}{d_{2,i_{o,v}1}} g^{r'_{i_{o,v}}}$。可以计算出 $\dfrac{d_{1,i_{o,v}0}}{d_{2,i_{o,v}0}} = g_2^{t_{1,o}(i_{o,v}) - t_{2,o}(i_{o,v})} H_1(i_{o,v})^{r_{1,i_{o,v}} - r_{2,i_{o,v}}}$，$\dfrac{d_{1,i_{o,v}1}}{d_{2,i_{o,v}1}} = g^{r_{1,i_{o,v}} - r_{2,i_{o,v}}}$。设 $r''_{i_{o,v}} = r_{1,i_{o,v}} - r_{2,i_{o,v}} + r'_{i_{o,v}}$，($d$−1)次多项式 $t''_o(i_{o,v}) = t_{1,o}(i_{o,v}) - t_{2,o}(i_{o,v}) + t'_o(i_{o,v})$，且 $t''_o(0) = 0$，则 $\sigma^*_{1,i_{o,v}1} = d_{2,i_{o,v}0} \quad H_1(i_{o,v})^{r''_{i_{o,v}}} g_2^{t''_o(i_{o,v})} \quad H_2(w^*)^{s_{i_{o,v}}}$，$\sigma^*_{1,i_{o,v}2} = d_{2,i_{o,v}1} g^{r''_{i_{o,v}}}$。因此，由密钥 $\mathrm{sk}_{\hat{\omega}^*_{1,o}}$ 生成的授权也可以由密钥 $\mathrm{sk}_{\hat{\omega}^*_{2,o}}$ 生成。类似地，可得由密钥 $\mathrm{sk}_{\hat{\omega}^*_{2,o}}$ 生成的授权也可以由密钥 $\mathrm{sk}_{\hat{\omega}^*_{1,o}}$ 生成。因此，A 赢得该游戏的优势是可忽略的，所提 ABPS 方案保护了原始签名者的隐私。定理 4 证毕。

定理 5 本文提出的 ABPS 方案保护了代理签名者的隐私。

证明 采用与定理 4 类似的证明方法，可证明本文提出的 ABPS 方案保护了代理签名者的隐私。

挑战者 C 选择安全参数，生成公开参数 params 和主密钥 α，并将(params, α)发送给敌手 A。A 计算出密钥 $\mathrm{sk}_{\hat{\omega}^*_{u,p}} = (d_{u,i_{p,\hat{v}}0}, d_{u,i_{p,\hat{v}}1})$。其中，$d_{u,i_{p,\hat{v}}0} = g_2^{t_{u,p}(i_{p,\hat{v}})} H_1(i_{p,\hat{v}})^{r_{u,i_{p,\hat{v}}}}$，$d_{u,i_{p,\hat{v}}1} = g^{r_{u,i_{p,\hat{v}}}}$，$t_{u,p}(\cdot)$ 是(d−1)次多项式且 $t_{u,p}(0) = \alpha$，$\hat{\omega}^*_{u,p} = \omega^*_{u,p} \cup \Omega$，$i_{p,\hat{v}} \in \hat{\omega}^*_{u,p}$，$1 \leqslant \hat{v} \leqslant |\hat{\omega}^*_{u,p}|$，$u \in \{1,2\}$，随机数 $r_{u,i_{p,\hat{v}}} \in Z_q$。

A 收到授权 $(\sigma_{i_o}1, \sigma_{i_{o,v}2}, \sigma_{i_{o,v}3})$ 后，选择消息 m^* 和属性集 ω^*_p，且 $\omega^*_p \subseteq \omega^*_{1,p} \cap \omega^*_{2,p}$，$|\omega^*_p| = k_p \leqslant d$。C 随机选择 $u \in \{1,2\}$，$\Omega'_p \subseteq \Omega$ 且 $|\Omega'_p| = d - k_p$，$r'_{i_{p,v}}, s_{i_{p,v}} \in Z_q$ 且 $i_{p,v} \in \omega^*_p \cup \Omega'_p$，$1 \leqslant v \leqslant d$。计算出签名 $(\sigma^*_{u,i_p1}, \sigma^*_{u,i_{p,v}2}, \sigma^*_{u,i_{p,v}3}, \sigma^*_{u,i_{p,v}4}, \sigma^*_{u,i_{p,v}5})$。将由密钥 $\mathrm{sk}_{\hat{\omega}^*_{1,p}}$ 生成的签名 σ^*_{1,i_p1} 中的 $\sigma^*_{1,i_{p,v}1}$ 和 $\sigma^*_{1,i_{p,v}2}$ 写成 $\sigma^*_{1,i_{p,v}1} = d_{2,i_{p,v}0} H_1(i_{p,v})^{r''_{i_{p,v}}} g_2^{t''_p(i_{p,v})} H_3(m^*)^{s_{i_{p,v}}}$，$\sigma^*_{1,i_{p,v}2} = d_{2,i_{p,v}1} g^{r''_{i_{p,v}}}$。其中，$r''_{i_{p,v}} = r_{1,i_{p,v}} - r_{2,i_{p,v}} + r'_{i_{p,v}}$，($d$−1) 次多项式 $t''_p(i_{p,v}) = t_{1,p}(i_{p,v}) - t_{2,p}(i_{p,v}) + t'_p(i_{p,v})$，且 $t''_p(0) = 0$。因此，由密钥 $\mathrm{sk}_{\hat{\omega}^*_{1,p}}$ 生成的签名也可以由密钥 $\mathrm{sk}_{\hat{\omega}^*_{2,p}}$

生成。类似地，可得由密钥 $\mathrm{sk}_{\hat{\omega}^*_{2,p}}$ 生成的签名也可以由密钥 $\mathrm{sk}_{\hat{\omega}^*_{1,p}}$ 生成。因此，A 赢得该游戏的优势是可忽略的，所提 ABPS 方案保护了代理签名者的隐私。定理 5 证毕。

根据定理 4 和定理 5，可得本文提出的 ABPS 方案保护了签名者的隐私。

6.4　效率分析

本文从计算开销和通信开销 2 个方面对所提 ABPS 方案和 ABPS-LXM 方案[19]、ABPS-SCX 方案[20]进行分析对比。对于计算开销，为反映无人机执行命令的实时性，本文主要分析了 Sign 和 Verify 算法的计算耗时。计算耗时越短，则计算开销越小，无人机执行命令的实时性越高。对于通信开销，主要分析了签名的长度。签名长度越短，则通信开销越小。考虑到无人机网络的实际应用状况，选取了较少的属性进行研究。

6.4.1　计算开销

本节简要分析了不同签名方案中 Sign 和 Verify 算法包含的一些基本运算量，主要包括幂运算、hash 运算和双线性映射运算。在所提 ABPS 方案的 Sign 算法中，计算 $\sigma_{i_{p,1}}$ 需要进行 $4d$ 次幂运算和(d+1)次 hash 运算，计算 $\sigma_{i_{p,v}2}$ 需要进行 d 次幂运算，计算 $\sigma_{i_{p,v}3}$ 和 $\sigma_{i_{p,v}4}$ 不需要额外运算，计算 $\sigma_{i_{p,v}5}$ 需要进行 d 次幂运算。因此，在 Sign 算法中，总共需要进行 $6d$ 次幂运算和(d+1)次 hash 运算。采用同样的方法对 Verify 算法进行分析，可计算出总共需要 $2d$ 次幂运算，(2d+2)次 hash 运算和(4d+1)次双线性映射运算。类似地，可以得出 ABPS-LXM 和 ABPS-SCX 方案中所需的计算量。分析结果如表 1 和表 2 所示。

表 1　不同签名方案中 Sign 算法的基本运算量

签名方案	幂运算	hash 运算	双线性映射
所提 ABPS 方案	6d	d+1	0
ABPS-LXM 方案	(n+4)(n+d−k)+2d+4	0	0
ABPS-SCX 方案	2	1	0

表 2　不同签名方案中 Verify 算法的基本运算量

签名方案	幂运算	hash 运算	双线性映射
所提 ABPS 方案	2d	2d+2	4d+1
ABPS-LXM 方案	2(n+2) (n+d−k)	0	2(n+d−k)+3
ABPS-SCX 方案	(n+3)d	2	3d+2

实验所用计算机的 CPU 为 Intel i5-4590。为了便于研究和表述，假设文献[19]中 n=d=2k，文献[20]中 n=d，S_A=S_B。在实验数据的基础上，可以估算出不同签名方案中 Sign 和 Verify 算法的计算耗时，如图 3 和图 4 所示。从图 3 和图 4 中可以发现，与 ABPS-LXM 方案相比，所提 ABPS 方案的 Sign 和 Verify 算法明显具有更少的计算开销。与 ABPS-SCX 相比，所提 ABPS 方案的 Sign 算法的计算开销稍大，这是由于 ABPS-SCX 方案在 Sign 算法之前添加了代理密钥生成算法，并将大量的计算放在了该算法中，从而降低了 Sign 算法的计算开销，而所提 ABPS 方案和 ABPS-LXM 方案都没有在 Sign 算法之前添加代理密钥生成算法；与 ABPS-SCX 方案相比，所提 ABPS 方案的 Verify 算法明显具有更少的计算开销。总体而言，所提 ABPS 方案具有更少的计算开销。

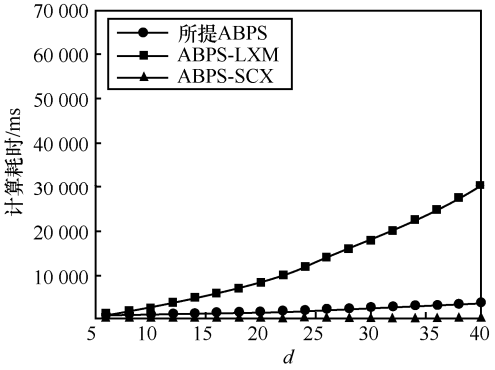


图 3　不同签名方案中 Sign 算法的计算耗时

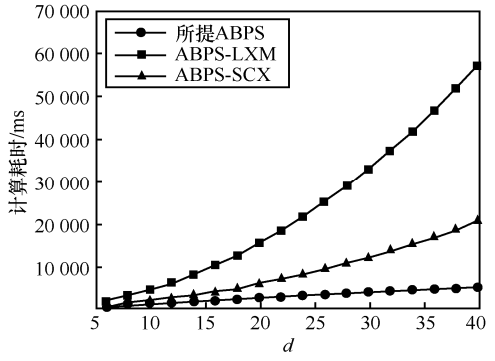


图 4　不同签名方案中 Verify 算法的计算耗时

本文采用 jPBC（Java pairing based cryptography）[21]实现了上述基本运算，获取了这些基本运算的计算耗时，如表 3 所示。

表 3　　基本运算的计算耗时

基本运算	计算耗时/ms
幂运算	11.11
hash 运算	29.28
双线性映射	11.38

6.4.2 通信开销

本节对所提 ABPS 方案、ABPS-LXM 方案和 ABPS-SCX 方案的签名长度进行了分析，如表 4 所示。从表 4 中可以发现，所提 ABPS 方案的签名长度与 ABPS-LXM 方案和 ABPS-SCX 方案的签名长度在同一水平。

表 4 不同签名方案的签名长度

签名方案	签名长度
所提 ABPS 方案	$(4d+1)\ \|G\|$
ABPS-LXM 方案	$(2(n+d-k)+3)\|G\|$
ABPS-SCX 方案	$(3d+2)\|G\|$

7 结束语

无人机在执行远程任务时，需要采用数字签名保护发送给无人机的命令，而且要保证无人机能及时收到命令和签名，保护签名者的隐私。因此，本文提出了面向无人机网络的属性代理签名方案，并对其安全性和效率进行了分析。该签名方案在选择属性和选择消息攻击下具有存在的不可伪造性，而且能保护签名者的隐私。从计算开销和通信开销两方面将所提方案与其他方案进行了对比。结果表明，所提方案的计算开销较小，通信开销与其他方案在同一水平。

参考文献：

[1] GUPTA L, JAIN R, VASZKUN G. Survey of important issues in UAV communication networks[J]. IEEE Communications Surveys & Tutorials, 2016, 18(2):1123-1152.

[2] MAJI H K, PRABHAKARAN M, ROSULEK M. Attribute-based signatures[C]//2011 Cryptographers' Track at the RSA Conference. Berlin: Springer, 2011: 376-392.

[3] LI J, KIM K. Hidden attribute-based signatures without anonymity revocation[J]. Information Sciences, 2010, 180(9):1681-1689.

[4] LI J, AU M H, SUSILO W, et al. Attribute-based signature and its applications[C]//Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2010: 60-69.

[5] 莫若, 马建峰, 刘西蒙, 等. 一种支持树形访问结构的属性基可净化签名方案[J]. 电子学报, 2017, 45(11): 2715-2720.
MO R, MA J F, LIU X M, et al. An attribute-based sanitizable signature supporting dendritic access structure[J]. Acta Electronica Sinica, 2017, 45(11): 2715-2720.

[6] GU K, JIA W J, WANG G J, et al. Efficient and secure attribute-based signature for monotone predicates[J]. Acta Informatica, 2017, 54(5): 521-541.

[7] 莫若, 马建峰, 刘西蒙, 等. 支持树形访问结构的多权威基于属性的签名方案[J]. 通信学报, 2017, 38(7): 96-104.
MO R, MA J F, LIU X M, et al. Multi-authority ABS supporting dendritic access structure[J]. Journal on Communications, 2017, 38(7): 96-104.

[8] GUO R, SHI H X, ZHAO Q L, et al. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems[J]. IEEE Access, 2018, 6: 11676-11686.

[9] YANG R L, CHEN J G, LI S L. Secure and traceable attribute-based sequential aggregate signature[C]//2020 International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Berlin: Springer, 2020: 367-381.

[10] CHEN X F, LI J, HUANG X Y, et al. Secure outsourced attribute-based signatures[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(12): 3285-3294.

[11] MO R, MA J F, LIU X M, et al. EOABS: expressive outsourced attribute-based signature[J]. Peer-to-Peer Networking and Applications, 2018, 11(5): 979-988.

[12] CUI H, DENG R H, LIU J K, et al. Server-aided attribute-based signature with revocation for resource-constrained industrial-Internet-of-things devices[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3724-3732.

[13] XIONG H, BAO Y Y, NIE X Y, et al. Server-aided attribute-based signature supporting expressive access structures for industrial Internet of things[J]. IEEE Transactions on Industrial Informatics, 2020, 16(2): 1013-1023.

[14] 张应辉, 贺江勇, 郭瑞, 等. 工业物联网中服务器辅助且可验证的属性基签名方案[J]. 计算机研究与发展, 2020, 57(10): 2177-2187.
ZHANG Y H, HE J Y, GUO R, et al. Server-aided and verifiable attribute-based signature for Industrial Internet of things[J]. Journal of Computer Research and Development, 2020, 57(10): 2177-2187.

[15] BAO Y Y, QIU W D, CHENG X C. Efficient and fine-grained signature for IIoT with resistance to key exposure[J]. IEEE Internet of Things Journal, 2021, 8(11): 9189-9205.

[16] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures for delegating signing operation[C]//Proceedings of the 3rd ACM Conference on Computer and Communications Security. New York: ACM Press, 1996: 48-57.

[17] HUANG X Y, SUSILO W, MU Y, et al. Proxy signature without random oracles[C]//2006 2nd International Conference on Mobile Ad-Hoc and Sensor Networks. Berlin: Springer, 2006: 473-484.

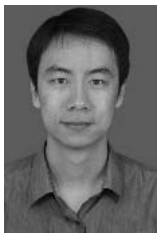
[18] WU W, MU Y, SUSILO W, et al. Identity-based proxy signature from pairings[C]//2007 4th International Conference on Autonomic and Trusted Computing. Berlin: Springer, 2007: 22-31.

[19] LIU X M, MA J F, XIONG J B, et al. Personal health records integrity verification using attribute-based proxy signature in cloud computing[C]//2013 6th International Conference on Internet and Distributed Computing Systems. Berlin: Springer, 2013: 238-251.

[20] SUN C X, GUO Y F, LI Y L. One secure attribute-based proxy signature[J]. Wireless Personal Communications, 2018, 103(2): 1273-1283.

[21] CARO A D, IOVINO V. jPBC: Java pairing based cryptography[C]//2011 IEEE Symposium on Computers and Communications. Piscataway: IEEE Press, 2011: 850-855.

[作者简介]



贺蕾（1980− ），男，山西平遥人，西安电子科技大学博士生，主要研究方向为应用密码学、无线网络安全等。

马建峰（1963− ），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为应用密码学、无线网络安全、数据安全、移动智能系统安全等。

魏大卫（1994− ），男，河北石家庄人，西安电子科技大学博士生，主要研究方向为无人机网络与系统安全等。