(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107733649 B
(45)授权公告日 2020.05.22

(21)申请号 201711168189.5

(22)申请日 2017.11.21

(65)同一申请的已公布的文献号
申请公布号 CN 107733649 A

(43)申请公布日 2018.02.23

(73)专利权人 武汉珈港科技有限公司
地址 430079 湖北省武汉市洪山区珞南街武珞路717#兆富国际大厦1栋16层11号

(72)发明人 涂航 彭聪 李莉 何德彪 宋奕

(74)专利代理机构 武汉科皓知识产权代理事务所(特殊普通合伙) 42222
代理人 魏波

(51)Int.Cl.
H04L 9/30(2006.01)

(56)对比文件
CN 105187205 A,2015.12.23,
CN 101471776 A,2009.07.01,
US 2008056501 A1,2008.03.06,
US 2012233457 A1,2012.09.13,
陈义涛.基于椭圆曲线的认证密钥协商协议的研究及应用.《中国博士学位论文全文数据库》.2015,
Debiao He;Huaqun Wang;Muhammad Khurram Khan;Lina Wang.Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography.《IET Communications》.2016,

审查员 刘莎莎

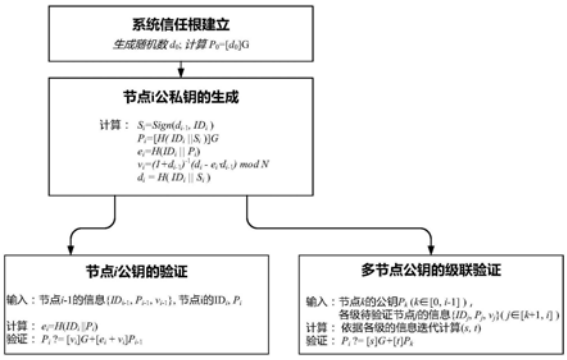
权利要求书2页 说明书5页 附图4页

(54)发明名称

一种基于身份标识的层级化公钥信任模型构建方法

(57)摘要

本发明公开了一种基于身份标识的层级化公钥信任构建方法,包括:基于ECC算法的系统信任根的建立;下级节点公私钥对及验证参数的生成方法;基于上级可信节点的节点公钥与身份标识绑定验证方法;基于可信节点与信任链关系的节点公钥与身份标识绑定验证方法;同时,支持素数扩域上的ECC算法。本发明实现了基于身份标识密码算法中的公钥与身份信息的绑定与验证,大大降低了使用传统公钥证书绑定用户身份带来的管理成本、资源消耗方面的负担。



CN 107733649 B

1.一种基于身份标识的层级化公钥信任模型构建方法,其特征在于,包括以下步骤:

步骤1:根据椭圆曲线密码算法的曲线参数{q,a,b,G,N}随机生成根公私钥对,其中q是一个用于构建有限域F_q的奇素数或2的方幂,a,b为F_q中的元素,它们定义F_q上的一条椭圆曲线,G表示椭圆曲线的一个基点,其阶为N;

步骤1的具体实现包括以下子步骤:

步骤1.1:确定椭圆曲线密码算法的5个曲线参数{q,a,b,G,N};

步骤1.2:根节点随机产生私钥d_0,计算公钥$P_0=[d_0]\cdot G$;其中根节点记为节点0;

步骤2:上级节点根据下级节点身份标识随机生成下级节点的公私钥对以及验证参数;

步骤2的具体实现包括以下子步骤:

步骤2.1:上级节点记为第i-1级节点,下级节点记为第i级节点,i为大于零的整数;上级节点使用自身的私钥d_{i-1}对下级节点的身份标识ID_i及其它附加信息签名,得到签名值S_i;

步骤2.2:上级节点计算下级节点的私钥$d_i=H(ID_i||S_i)$,公钥$P_i=[H(ID_i||S_i)]G$;

步骤2.3:上级节点计算下级节点的公钥验证参数$v_i=(1+d_{i-1})^{-1}(d_i-e_i\cdot d_{i-1})\bmod N$,其中$e_i=H(ID_i||P_i)$;

步骤2.4:上级节点将下级节点的注册信息$\{S_i,ID_i,P_i,v_i\}$安全的发送给下级节点;

步骤2.5:下级节点根据S_i生成自身的私钥$d_i=H(ID_i||S_i)$,公开下级节点的公钥信息$\{ID_i,P_i,v_i\}$;

步骤3:节点公钥验证,包括节点公钥单次验证和节点公钥级联验证;

所述节点公钥单次验证,是根据上级节点的公钥与下级节点的身份标识验证下级节点的公钥合法性;具体实现包括以下子步骤:

步骤3A.1:验证方将需验证的节点记为第i级节点,信任其上级节点的公钥P_{i-1},获取被验证节点的公开信息$\{ID_i,P_i,v_i\}$;

步骤3A.2:验证方计算$e=H(ID_i||P_i)$、$s=v_i$、$t=e+v_i$;

步骤3A.3:验证方验证等式$P_i=[s]G+[t]P_{i-1}$是否成立;若成立,则验证通过;否则,验证失败;

所述节点公钥级联验证,是根据信任链上各级节点的公钥及验证参数与下级节点的身份标识验证下级节点的公钥合法性;具体实现包括以下子步骤:

步骤3B.1:验证方将需验证的节点记为第i级节点,信任从第0级到第k级节点的公钥P_k,k为小于i的整数,获取第k+1级节点到第i级节点间的各级节点的公开信息$\{ID_j,P_j,v_j\}$,$j\in[k+1,i]$;

步骤3B.2:验证方执行以下计算:令$e=H(ID_i||P_i)$、$s=v_i$、$t=e+v_i$、$j=i-1$,当$j>k$时依序循环计算$e=H(ID_j||P_j)$、$s=s+t\cdot v_j$、$t=t\cdot(e+v_j)$、$j=j-1$,直到$j=k$时结束循环;

步骤3B.3:验证方验证等式$P_i=[s]G+[t]P_k$是否成立;若成立,则验证通过;否则,验证失败。

2.根据权利要求1所述的基于身份标识的层级化公钥信任模型构建方法,其特征在于:所述方法支持素数扩域上的公钥生成与验证,具体实现过程是椭圆曲线点选择坐标x'时,仅选取坐标一个多项式基的坐标参与运算。

3.根据权利要求1所述的基于身份标识的层级化公钥信任模型构建方法,其特征在于:根据节点公钥生成与验证方法建立层级化的IBC信任体系,任意IBC用户可以验证任一信任

节点系统公钥的合法性；

具体实现包括以下子步骤：

步骤C.1：建立一个KDC，作为信任根节点，规定IBC所用椭圆曲线参数，完成自身系统私钥和公钥的生成；

步骤C.2：由上级KDC生成下级KDC的系统私钥和公钥，私钥和公钥符合IBC算法运算要求；

步骤C.3：用户在获取公开信息的前提下，验证某一KDC的系统公钥的合法性，实现跨域信任。

一种基于身份标识的层级化公钥信任模型构建方法

技术领域

[0001] 本发明属于信息安全技术领域，具体涉及一种基于身份标识的层级化公钥信任模型构建方法。

背景技术

[0002] 伴随着信息技术的快速发展，移动通信网络、移动IP网络、无线传感器网络、物联网等新的网络形式得到迅速发展。为了保证通信与业务的安全，基于公钥密码算法的数字签名与认知技术得到了广泛的应用。

[0003] 1976年，Diffie和Hellman提供公钥密钥体制的概念，之后公钥密钥技术得到了广泛的发展，学者们提出了许多代表性的公钥密码算法：包括RSA算法、椭圆曲线密码ECC算法等。由于密码算法是公开的，因此确保公钥密码算法应用安全性主要依赖于私钥的保密性和可认证性。所以，公钥密码体制中存在一个非常重要的问题：如何建立一种用户身份、私钥与公钥三者间的保障关系。

[0004] 在传统公钥密码体制中，这种保障关系是以证书认证的形式提供，即由认证中心通过对公钥及身份信息的签名来完成，一般称这种认证形式为基于证书的公钥密码体制(Certificate-Based Public Key Cryptography，CA-PKC)。在CA-PKC中，公钥证书的申请、颁发与管理是一项非常复杂的任务。而且，公钥证书在使用过程中的传递、验证大大地提升了认证所需的资源消耗。除此之外，为建立证书信任体系而部署的公钥基础设施(Public Key Infrastructure，PKI)在建设、运行、维护等方面也带来了巨大的人力、物力、成本消耗。在物联网、移动通信等资源受限环境中，PKI存在的问题变得较为敏感。

[0005] 为了消除传统公钥密码体制中的公钥证书管理问题，Shamir于1984年提出了基于身份标识的公钥密码体制(IBC)，建立了“身份标识即用户公钥”的概念。直到2001年，Boneh和Franklin利用双线性对运算成功地构建了基于身份的有效加密算法。IBC在解决证书管理问题的同时，也引入了密钥托管的问题，使得系统安全极大地依赖于系统私钥的保密性。在实际使用时，为有效限制系统风险的危害范围，不同的信息系统间采用不同的KDC生成的系统参数(系统私钥与系统公钥)，形成了不同的信任域。不可避免的，不同信任域间存在着信息交互的可能。然而，不同域间用户相互信任的前提是信任双方的系统KDC。那么，如何让域内用户信任其它信任域的系统KDC是ID-PKC自身未解决的问题。较为传统的实现方式是：所有系统用户信任一个根KDC；上级KDC给下级KDC签发系统公钥证书；用户依次验证节点KDC的系统公钥证书，进而信任不同域的KDC。这种方式依旧采用了基于证书管理的思想，使得跨域环境下存在证书使用管理的问题。而且，双线性对的运算时间和空间复杂度较高，使得ID-PKC的运算效率成倍的低于传统公钥密码算法，较大地限制了其应用范围。

发明内容

[0006] 为了解决上述技术问题，本发明提供了一种可基于身份标识进行认证的公钥生成与验证方法，本发明在验证中既不采用基于证书密码体制，也不采用基于身份标识的密码

体制，减少验证公钥带来的计算量和通信量，做到安全、高效的验证公钥；本发明可用于建立计算量低、实用性强的层级化公钥信任体系。

[0007] 本发明所采用的技术方案是：一种基于身份标识的层级化公钥信任模型构建方法，其特征在于，包括以下步骤：

[0008] 步骤1：根据椭圆曲线密码算法的曲线参数{q,a,b,G,N}随机生成根公私钥对，其中q是一个用于构建有限域F_q的奇素数或2的方幂，a,b为F_q中的元素，它们定义F_q上的一条椭圆曲线，G表示椭圆曲线的一个基点，其阶为N；

[0009] 具体实现包括以下子步骤：

[0010] 步骤1.1：确定椭圆曲线密码算法的5个参数{q,a,b,G,N}；

[0011] 步骤1.2：根节点随机产生私钥d_0，计算公钥$P_0=[d_0]\cdot G$。

[0012] 步骤2：上级节点根据下级节点身份标识随机生成下级节点的公私钥对以及验证参数；

[0013] 具体实现包括以下子步骤：

[0014] 步骤2.1：上级节点，记为第i-1级节点(i为大于零的整数)，使用自身的私钥d_{i-1}对下级节点(记为第i级节点)的身份标识ID_i及其它附加信息签名，得到签名值S_i；

[0015] 步骤2.2：上级节点计算下级节点的私钥$d_i=H(PD_i||S_i)$，公钥$P_i=[H(ID_i||S_i)]G$；

[0016] 步骤2.3：上级节点计算下级节点的公钥验证参数$v_i=(1+d_{i-1})^{-1}(d_i-e_i\cdot d_{i-1}) \bmod N$，其中$e_i=H(ID_i||P_i)$；

[0017] 步骤2.4：上级节点将下级节点的注册信息$\{S_i,ID_i,P_i,v_i\}$安全的发送给下级节点；

[0018] 步骤2.5：下级节点根据S_i生成自身的私钥$d_i=H(ID_i||S_i)$，公开下级节点的公钥信息$\{ID_i,P_i,v_i\}$。

[0019] 步骤3：节点公钥验证，包括节点公钥单次验证和节点公钥级联验证。

[0020] 所述节点公钥单次验证，是根据上级节点的公钥与下级节点的身份标识验证下级节点的公钥合法性；具体实现包括以下子步骤：

[0021] 步骤3A.1：验证方将需验证的节点记为第i级节点(i为大于零的整数)，信任其上级节点的公钥P_{i-1}，获取被验证节点的公开信息$\{ID_i,P_i,v_i\}$；

[0022] 步骤3A.2：验证方计算$e=H(ID_i||P_i)$、$s=v_i$、$t=e+v_i$；

[0023] 步骤3A.3：验证方验证等式$P_i=[s]G+[t]P_{i-1}$是否成立；若成立，则验证通过；否则，验证失败。

[0024] 所述节点公钥级联验证，是根据信任链上各级节点的公钥及验证参数与下级节点的身份标识验证下级节点的公钥合法性；具体实现包括以下子步骤：

[0025] 步骤3B.1：验证方将需验证的节点记为第i级节点(i为大于零的整数)，信任从第0级到第k级节点的公钥P_k(k为小于i的整数)，获取第k+1级节点到第i级节点间的各级节点的公开信息$\{ID_j,P_j,v_j\}$，$j\in[k+1,i]$；

[0026] 步骤3B.2：验证方执行以下计算：令$e=H(ID_i||P_i)$、$s=v_i$、$t=e+v_i$、$j=i-1$，当$j>k$时依序循环计算$e=H(ID_j||P_j)$、$s=s+t\cdot v_j$、$t=t\cdot(e+v_j)$、$j=j-1$，直到$j=k$时结束循环；

[0027] 步骤3B.3：验证方验证等式$P_i=[s]G+[t]P_k$是否成立；若成立，则验证通过；否则，验证失败。

[0028] 本发明的有益效果是:由于本发明未采用证书体制,减少证书使用附加的计算量、通信量;仅使用椭圆曲线运算,避免采用双线性对运算带来的计算量增加的问题;仅提供了公钥生成与验证方法,公钥与私钥间具备传统的映射关系,可扩展兼容各种基于椭圆曲线的签名/验签、加密/解密、密钥协商方法;非常适用于构建层级化的IBC信任体系,并且降低了系统私钥泄露的危害范围;提供了一种公钥级联验证方式,可以从一个可信节点认证下游任一级别节点的公钥合法性,其计算量几乎等同于一次于单次公钥验证所需计算量,远低于按级序验证带来的多次公钥验证计算量。

附图说明

[0029] 图1是本发明实施例的流程图;

[0030] 图2是本发明实施例中信任根建立的原理示意图;

[0031] 图3是本发明实施例中节点公私钥对生成的原理示意图;

[0032] 图4是本发明实施例中基于上级节点可信的节点公钥验证方法的原理示意图;

[0033] 图5是本发明实施例中基于可信节点与信任链关系的节点公钥验证方法的原理示意图。

具体实施方式

[0034] 为了便于本领域普通技术人员理解和实施本发明,下面结合附图及实施例对本发明作进一步的详细描述,应当理解,此处所描述的实施示例仅用于说明和解释本发明,并不用于限定本发明。

[0035] 请见图1,本发明提供的一种基于身份标识的层级化公钥信任模型构建方法,包括信任根建立、节点公私钥对生成、节点公钥验证、节点公钥级联验证。

[0036] 图2展示了信任根建立的详细流程。在初始化阶段,根节点定义系统参数,以有限域F_q上的椭圆曲线构建,并生成系统根公私钥对$\{d_0,P_0\}$。

[0037] 具体步骤如下:

[0038] 1)选取参数q(q为素数的m次方)和三次方程$y^2=x^3+ax+b$的参数a、b,确定椭圆曲线群$E_q(a,b)$,以及阶为N的元素$G=(x_G,y_G)$作为生成元,称为基点。由此确定椭圆曲线密码算法的5个参数$\{q,a,b,G,N\}$。

[0039] 2)根节点随机生成一个随机数$d_0\in[1,N-1]$作为系统根私钥,同时,计算系统根公钥$P_0=[d_0]G$。

[0040] 3)根节点公开q,a,b,G,N,P_0,秘密存储d_0。同时,选定一个安全的单向哈希函数,并确定一种比特序列映射到有限域的方法,记为$H(\bullet)$并公开。

[0041] 图3展示了节点公私钥对生成的详细流程。在节点公私钥对生成阶段,当前节点(含根节点)A_i根据下级节点A_{i-1}的身份标识ID_i生成下级节点的公私钥对$\{d_i,P_i\}$,其中私钥具备随机性和不可否认性(即能识别是否由上级节点分发)。

[0042] 具体步骤如下:

[0043] 1)A_i选取(或获取)下级节点的身份标识ID_i,使用自身的私钥d_{i-1}对ID_i及其它附加信息签名,得到签名值S_i。

[0044] 2)A_i计算下级节点的私钥$d_i=H(ID_i||S_i)$和公钥$P_i=[d_i]G$。

[0045] 3)A_i计算下级节点的公钥验证参数$v_i=(1+d_{i-1})^{-1}(d_i-e_i\cdot d_{i-1})\bmod N$,其中$e_i=H(ID_i||P_i)$。

[0046] 4)A_i将$\{S_i,ID_i,P_i,v_i\}$安全的发送给下级节点A_{i-1}。

[0047] 5)A_{i-1}根据S_i生成自身的私钥$d_i=H(ID_i||S_i)$,公开下级节点的公钥信息$\{ID_i,P_i,v_i\}$。

[0048] 图4展示了基于上级节点可信的节点公钥验证阶段的详细流程。在该节点公钥验证阶段,验证方可根据上级节点的公钥信息验证被验证节点公钥的合法性以及与身份标识的绑定关系。验证方式如下:

[0049] 1)验证方获取被验证节点的信息$\{ID_i,P_i,v_i\}$,及其上级节点的公钥P_{i-1};验证方信任上级节点。

[0050] 2)验证方计算$e_i=H(ID_i||P_i)$。

[0051] 3)验证方验证等式$P_i=[v_i]G+[e_i+v_i]P_{i-1}$是否成立;若成立,则验证通过;否则,验证失败。

[0052] 图5展示了基于可信节点与信任链关系的节点公钥验证阶段的详细流程。在节点公钥级联验证阶段,验证方可根据信任链上各级节点的公钥信息验证被验证节点公钥的合法性以及与身份标识的绑定关系。验证方式如下:验证方式如下:

[0053] 1)验证方将需验证的节点记为第i级节点(i为大于零的整数),信任从第0级到第k级节点的公钥P_k(k为小于i的整数),获取第k+1级节点到第i级节点间的各级节点的公开信息$\{ID_j,P_j,v_j\}$,$j\in[k+1,i]$。

[0054] 2)令$e=H(ID_i||P_i)$、$s=v_i$、$t=e+v_i$、$j=i-1$。

[0055] 3)若$j>k$,计算$e=H(ID_j||P_j)$、$s=s+t\cdot v_j$、$t=t\cdot(e+v_j)$、$j=j-1$;

[0056] 4)若$j=k$,则继续;否则,重复执行第3)步。

[0057] 5)验证方验证等式$P_i=[s]G+[t]P_k$是否成立;若成立,则验证通过;否则,验证失败。

[0058] 本发明支持素数扩域上的公钥生成与验证,方式如下:在上述计算步骤中,椭圆曲线点选择坐标x′时,仅选取坐标一个多项式基的坐标参与运算。

[0059] 本发明根据节点公钥生成与验证方法建立层级化的IBC(Identity Based Cryptograph,基于身份标识的密码)信任体系,任意IBC用户可以验证任一信任节点系统公钥的合法性;

[0060] 具体实现包括以下子步骤:

[0061] 步骤C.1:建立一个KDC(Key Distribution Center,密钥分发中心),作为信任根节点,规定IBC所用椭圆曲线参数,完成自身系统私钥和公钥的生成;

[0062] 步骤C.2:由上级KDC生成下级KDC的系统私钥和公钥,该密钥对符合IBC算法运算要求;

[0063] 步骤C.3:用户在获取公开信息的前提下,验证某一KDC的系统公钥的合法性,实现跨域信任。

[0064] 应当理解的是,本说明书未详细阐述的部分均属于现有技术。

[0065] 应当理解的是,上述针对较佳实施例的描述较为详细,并不能因此而认为是对本发明专利保护范围的限制,本领域的普通技术人员在本发明的启示下,在不脱离本发明权

利要求所保护的范围情况下，还可以做出替换或变形，均落入本发明的保护范围之内，本发明的请求保护范围应以所附权利要求为准。

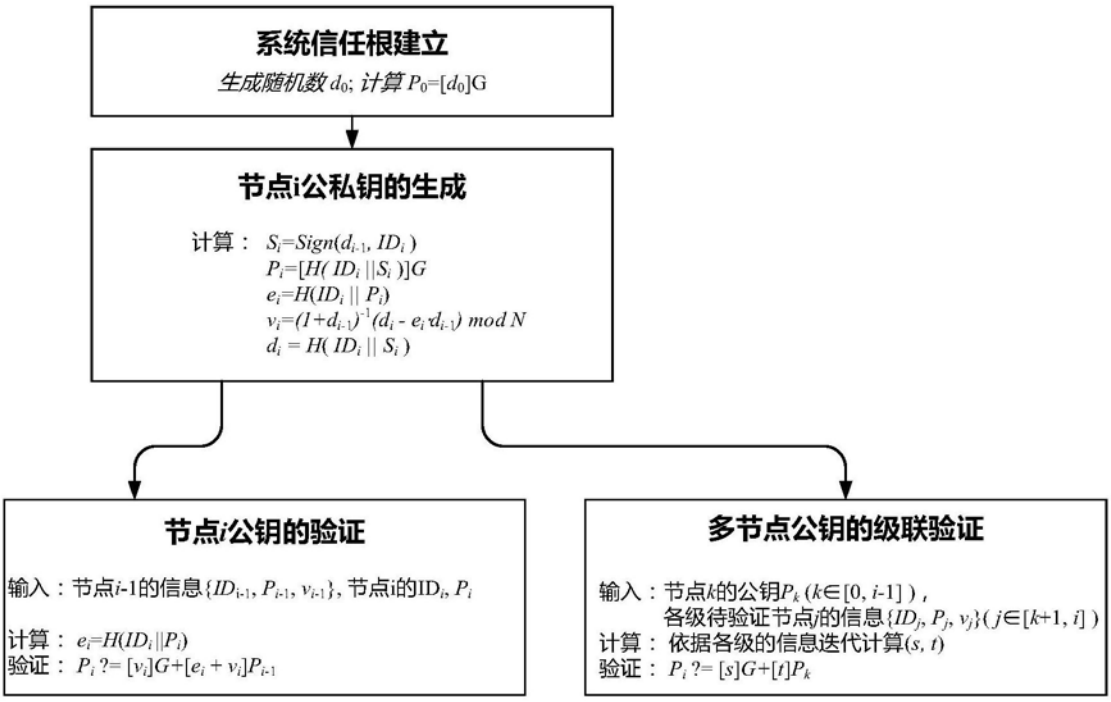

系统信任根建立
生成随机数 d_0; 计算 $P_0=[d_0]G$
节点i公私钥的生成
计算： $S_i=Sign(d_{i-1}, ID_i)$
$P_i=[H(ID_i||S_i)]G$
$e_i=H(ID_i||P_i)$
$v_i=(1+d_{i-1})^{-1}(d_i - e_i \cdot d_{i-1}) \bmod N$
$d_i = H(ID_i||S_i)$
节点i公钥的验证
输入：节点i-1的信息$\{ID_{i-1}, P_{i-1}, v_{i-1}\}$, 节点i的$ID_i$, P_i
计算： $e_i=H(ID_i||P_i)$
验证： $P_i ?= [v_i]G+[e_i + v_i]P_{i-1}$
多节点公钥的级联验证
输入：节点k的公钥P_k ($k\in[0, i-1]$)，
各级待验证节点j的信息$\{ID_j, P_j, v_j\}$ ($j\in[k+1, i]$)
计算： 依据各级的信息迭代计算(s, t)
验证： $P_i ?= [s]G+[t]P_k$

图1

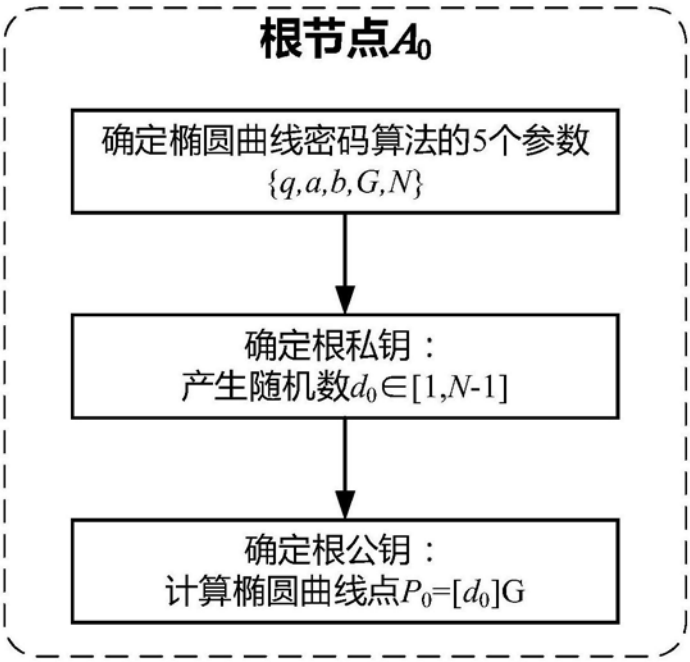

根节点A_0
确定椭圆曲线密码算法的5个参数
$\{q,a,b,G,N\}$
确定根私钥：
产生随机数$d_0\in[1,N-1]$
确定根公钥：
计算椭圆曲线点$P_0=[d_0]G$

图2

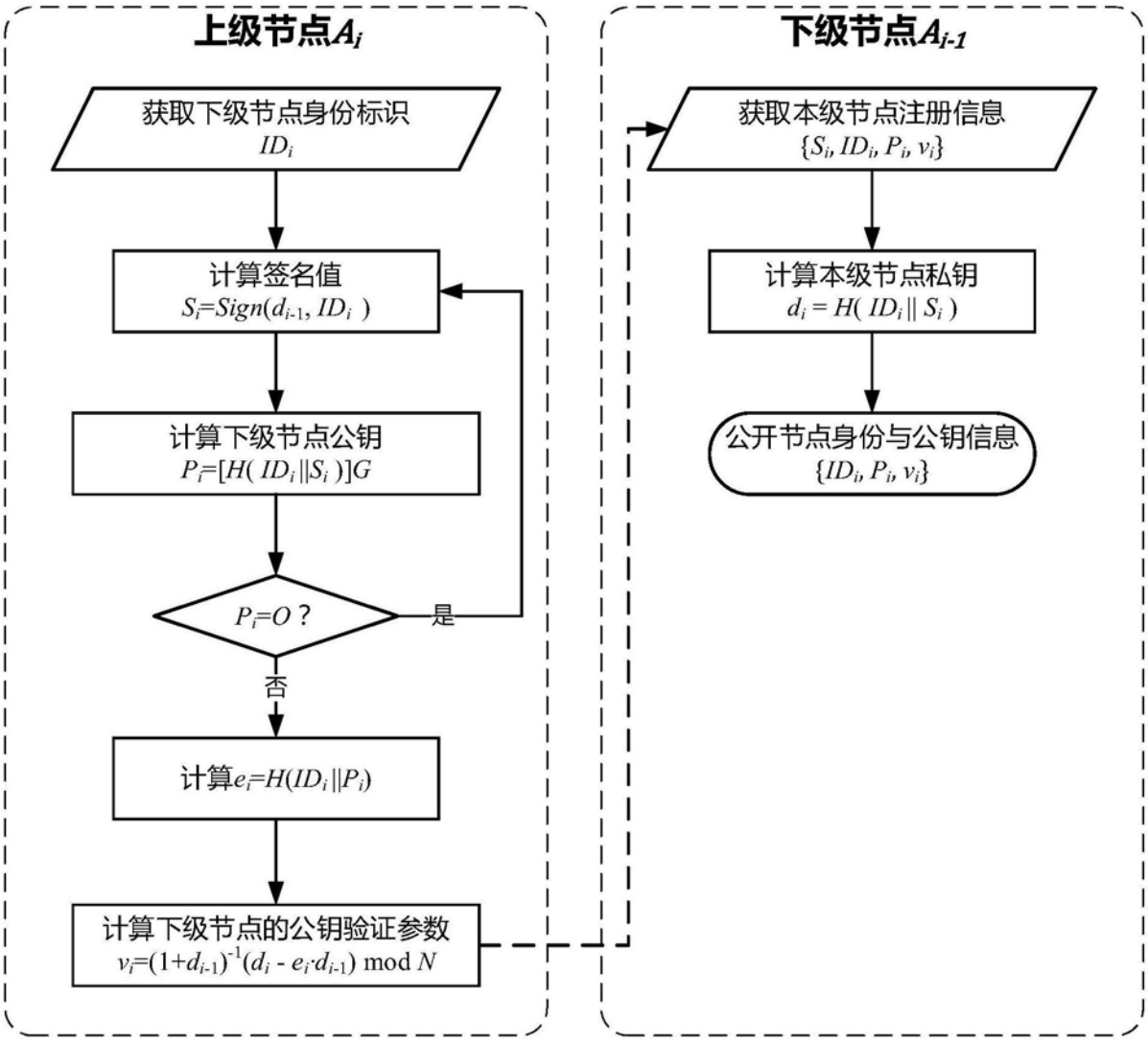

上级节点A_i
获取下级节点身份标识
ID_i
计算签名值
$S_i=Sign(d_{i-1}, ID_i)$
计算下级节点公钥
$P_i=[H(ID_i||S_i)]G$
$P_i=O$？
是
否
计算$e_i=H(ID_i||P_i)$
计算下级节点的公钥验证参数
$v_i=(1+d_{i-1})^{-1}(d_i - e_i \cdot d_{i-1}) \bmod N$
下级节点A_{i-1}
获取本级节点注册信息
$\{S_i, ID_i, P_i, v_i\}$
计算本级节点私钥
$d_i = H(ID_i || S_i)$
公开节点身份与公钥信息
$\{ID_i, P_i, v_i\}$

图3

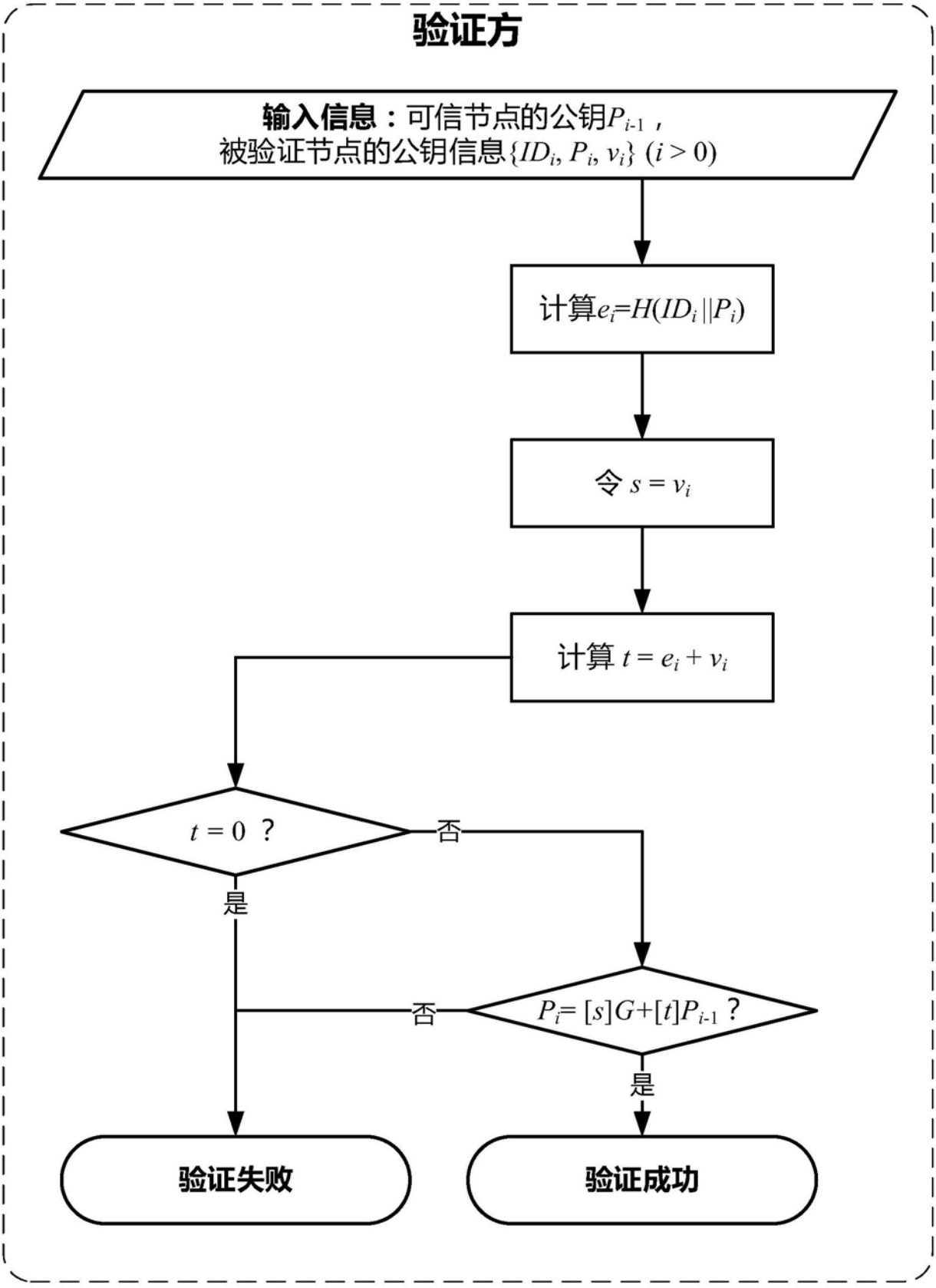

验证方
输入信息：可信节点的公钥P_{i-1}，
被验证节点的公钥信息$\{ID_i, P_i, v_i\}$ $(i > 0)$
计算$e_i=H(ID_i||P_i)$
令 $s = v_i$
计算 $t = e_i + v_i$
$t = 0$ ？
否
是
否
$P_i= [s]G+[t]P_{i-1}$ ？
是
验证失败
验证成功

图4

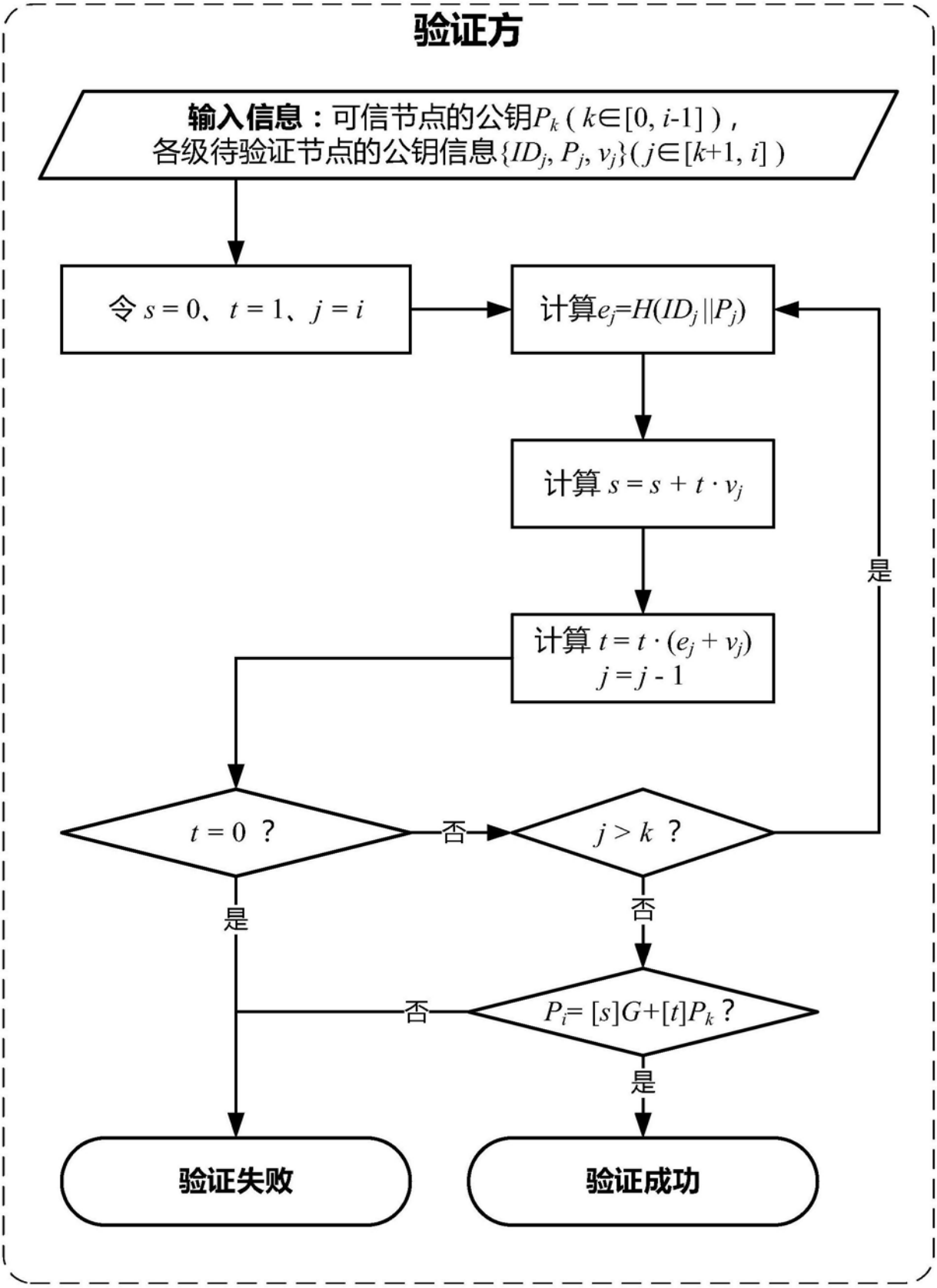

验证方
输入信息：可信节点的公钥P_k ($k\in[0, i\text{-}1]$) ，
各级待验证节点的公钥信息$\{ID_j, P_j, v_j\}$($j\in[k+1, i]$)
令 $s=0$、$t=1$、$j=i$
计算$e_j=H(ID_j \| P_j)$
计算 $s=s+t\cdot v_j$
计算 $t=t\cdot(e_j+v_j)$
$j=j-1$
$t=0$ ？
否
$j>k$ ？
是
是
否
否
$P_i=[s]G+[t]P_k$ ？
是
验证失败
验证成功

图5