基于双重代理密钥的船舶自组网门限签名方案

徐明[1]，李旭如[1]，刘朝斌[2]，马尧[3]

(1. 上海海事大学信息工程学院，上海 201306；2. 复旦大学上海市智能信息处理重点实验室，上海 200433；
3. 中国通用技术研究院，北京 100085)

摘 要：为了解决船舶自组网应用条件下的消息认证问题，利用门限代理签名体制和双线性对性质，设计了一种不依赖于可信认证中心和防篡改设备的签名方案。通过双重代理密钥的设计和门限签名机制的应用，使船舶节点通过多项式时间的计算完成消息签名，并运用随机预言模型证明了方案的安全性。分析表明，该方案在保证正确性的前提下能满足强代理签名的性质，并具有较低的计算开销和通信开销。

关键词：船舶自组网；双重代理密钥；消息认证；双线性对

中图分类号：TP309

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2018115

Dual-proxy key-based threshold signature scheme for ship ad-hoc network

XU Ming[1], LI Xuru[1], LIU Chaobin[2], MA Yao[3]

1. College of Information Engineering, Shanghai Maritime University, Shanghai 201306, China
2. Shanghai Key Laboratory of Intelligent Information Processing, Fudan University, Shanghai 200433, China
3. China General Technology Research Institute, Beijing 100085, China

Abstract: In order to solve the problem of message authentication under the conditions of the ship ad-hoc network (SANET), a signature scheme that does not depend on trusted certificate authorities and tamper-proof devices (TPD) was proposed by using the threshold proxy signature scheme and the properties of bilinear pairings. The proposed scheme used the dual-proxy key and the threshold signature mechanism to enable the ship nodes calculate the message signature in polynomial time. Moreover, the security of the scheme was also proved under the random oracle model. The performance analysis results show that the proposed scheme can meet the requirement of strong proxy signature under the premise of guaranteeing correctness, and has lower computational cost and communication cost.

Key words: ship ad-hoc network, dual-proxy key, message authentication, bilinear pairing

1 引言

船舶自组网（SANET , ship ad-hoc network）是船联网（IoV, Internet of vessel）的一种组网形式[1]。广义的船联网是包含船舶、通信基站、通信卫星、桥梁、航标、浮标和船舶交通管理系统（VTS, vessel traffic system）组成的船舶智能信息服务系统。现有的一些海上通信应用，如船舶自动定位系统（AIS, automatic identification system）、全球海上遇险安全系统（GMDSS, global maritime distress safety system）都致力于船舶的安全、追踪和身份识别[2-4]。随着海上通信应用环境的复杂化，目前较为成熟的

收稿日期：2017−10−04；**修回日期**：2018−05−25

通信作者：徐明，mingxu@shmtu.edu.cn

基金项目：国家自然科学基金资助项目（No.U1636205）；中国博士后科学基金资助项目（No.2014M561512）

Foundation Items: The National Natural Science Foundation of China (No.U1636205), China Postdoctoral Science Foundation Project (No.2014M561512)

通信技术，如海事卫星通信系统因其高昂的费用逐渐成为海上通信应用的瓶颈。与此同时，海上活动日渐频繁以及无线通信技术迅速发展，为船舶自组网迎来了新的发展契机[5]。目前，船舶自组网的研究工作主要集中在通信效率的提升和路由协议的优化与设计方面[6-8]。然而，由于海面环境复杂、海面粗糙度（SSR, sea surface roughness）[9]多变以及天气变换频繁等不确定因素的影响，加之船舶节点移动速度较慢、网络拓扑结构相对稳定等原因，导致船舶节点之间的消息通信很容易被探测、拦截和篡改[10]。因此，如何保证船舶自组网的安全通信成为一个不可忽视的问题。

与常见的移动自组网（ad-hoc）相比，船舶自组网有以下 3 个特点。1) 从网络的整体结构来看，船舶节点之间的距离相对较远、节点移动速度较慢且移动速度相对稳定，这就导致了船舶自组网的拓扑结构变化较慢。2) 海洋环境复杂多变、覆盖区域较大，从而使浮标、岛屿基站等网络基础设施建设较为困难。因此，当船舶节点间进行通信时，这些基础设施可能无法作为可信第三方加入通信以保证船舶之间的通信安全。3) 由于针对船舶自组网安全通信的研究刚刚起步，目前还没有针对船舶自组网消息认证方面的研究工作，为了进一步完善船舶自组网的安全通信协议，设计一个适用于船舶自组网的消息认证方案是很必要的。

考虑到船舶自组网的特殊应用环境和网络结构，为了保证网络通信的可靠性，船舶自组网的消息认证方案设计不能引入第三方可信中心。但是船舶自组网中节点移动速度较慢、通信半径较大（约 30 km）、传输速率较快（9.6~14.4 kbit/s）[11]，这就意味着网络对于瞬时通信的要求较低。结合船舶自组网消息认证方案设计的需求与网络自身的特点，通过对现有移动自组网消息认证方案的研究，可以考虑使用门限代理签名对船舶自组网中的消息进行认证。

代理签名自 Mambo 等[12]在 1996 年首次提出后就被广泛深入地研究，随后，Zhang 等[13]提出了基于秘密共享的门限代理签名方案。在此之后，大量的门限代理签名方案被提出[14-20]。门限代理签名方案利用秘密共享和公钥密码体制保证了签名的安全性，由于其对代理签名的参与者身份没有做特殊的要求，因此可以在不引入第三方可信中心的前提下实现安全的消息认证；同时，船舶自组网对瞬时通信要求较低，可以负担由秘密共享过程所增加的计算复杂度和通信复杂度。因此说，门限代理签名方案是保证船舶自组网安全通信的一个较为理想的方案。常见的移动自组网中也有与之相似的认证方案，如 Shao 等[21]提出的门限批量认证方案和 Yeh 等[22]提出的基于代理车辆的认证方案，但是这 2 种方案均局限于使用第三方可信中心。

针对船舶自组网的特性及其应用环境的特殊限制，本文设计了一种基于双重代理密钥的门限签名方案。该签名方案不依赖于第三方认证中心和固定的基础设施。理论分析表明，该方案满足强代理签名的性质，即强不可伪造性、强可识别性、强不可否认性和防滥用性[23]。此外，效率分析表明，本文方案在船舶自组网的应用环境下具有较高的计算效率和通信效率。

2　船舶自组网体系结构及攻击模型

2.1　体系结构

船舶自组网包含船舶通信单元、基础设施通信单元和通信基站，其体系结构如图 1 所示。

船舶通信单元（OBU, on-board unit）：OBU 是安装在船舶上的通信设备，是船舶自组网中最基本的通信实体。

无线接入基站（RAS, radio access station）：RAS 包含陆地通信基站和岛屿通信基站。船舶自组网中的 RAS 可以作为其他后备网络的接入点。船舶、航道、环境等数据通过互联网传入相应服务器，可以用于 VTS 的管理决策。

无线接入点（AP, access point）[22]：船舶自组网中的无线接入点包含航标、浮标和桥梁。通过装载在这些设备上的传感器可以完成对环境和航道参数的感知与监控，AP 可以通过船舶自组网传送监测到的航运和环境数据。当船只不在 RAS 的覆盖范围内时，可以通过 AP 间接加入网络。

甚高频带（VHFB, very high frequency band）通信技术：考虑到船舶自组网应用环境的特殊性，一般的通信技术，如专用短程通信（DSRC, dedicated short range communication）技术[24]等受到传输速率的制约，而卫星通信则存在着成本较高和通信时延较大等问题。因此，Hui 等[25]提出的基于 ITU-R-M.1842-1 标准的甚高频带通信技术适用于船舶自组网的通信。

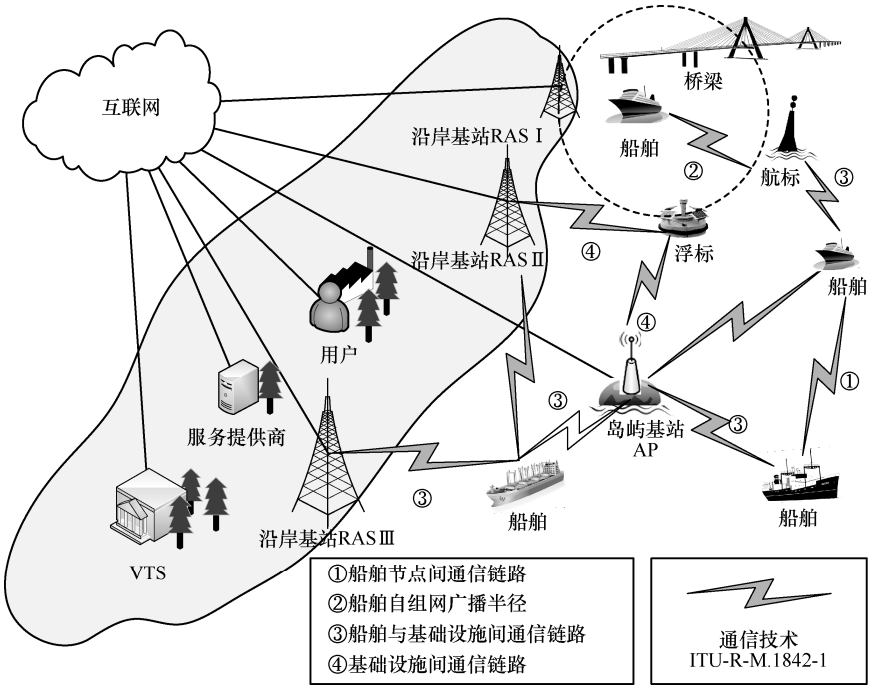


图 1 船舶自组网体系结构

2.2 攻击模型

针对船舶自组网的网络架构，有 3 种常见的攻击模型。图 2 给出了 3 种类型攻击者的攻击路径。

Ⅰ型攻击者可以窃听网络信道，从而获取对攻击者有利的消息。攻击者可以通过逆向分析技术得出原网络的消息格式、应答方式和容错机制等敏感信息。Ⅱ型攻击者通过对中继船舶节点 C 的消息进行拦截，并向接收船舶节点 B 发送篡改后的虚假消息以完成攻击目的。Ⅲ型攻击者通过向接入互联网的 RAS 和 AP 注入恶意代码，从而控制网络流量。其中，Ⅱ型攻击者的攻击模式尤为常见。而基于双重代理密钥的门限代理签名方案为船舶自组网中的消息认证提供了一种安全有效的解决方案。

3 基于双重代理密钥的门限签名方案

船舶自组网中门限代理签名方案的工作过程如图 3 所示。船舶节点 A 是原始签名人，它向代理

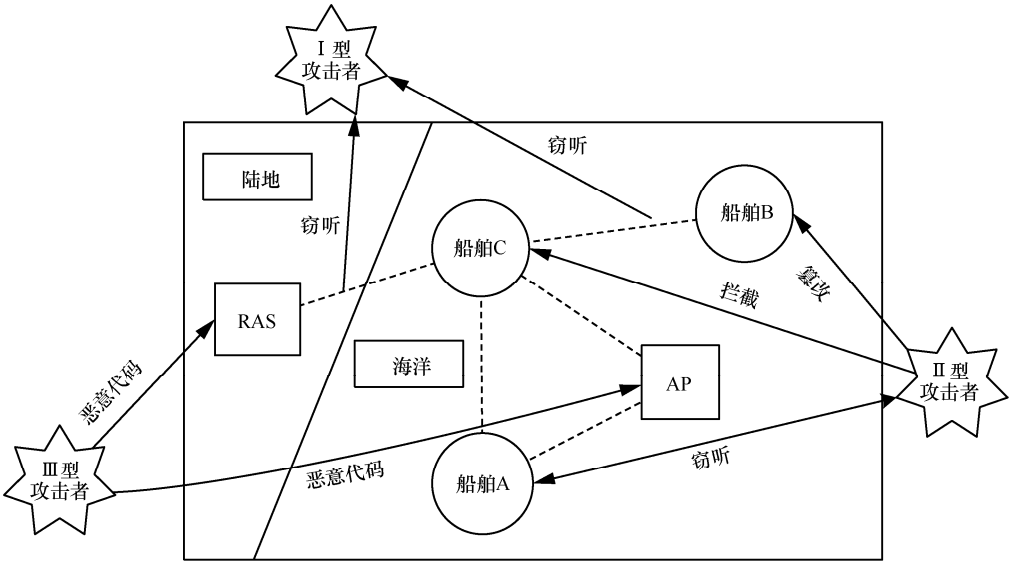


图 2 船舶自组网的攻击路径

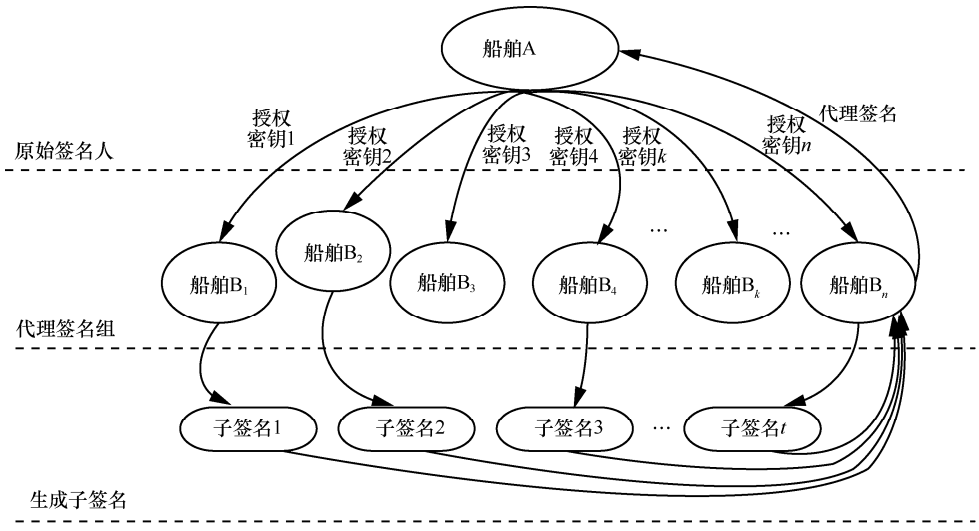


图 3　船舶自组网代理签名过程

签名组中的 n 个代理船舶节点发送授权密钥。其中，t 个船舶节点产生子签名，并交由一个签名管理节点汇总后返回给船舶节点 A。产生签名和签名管理的节点在代理签名节点中随机选举，并且整个签名过程只有船舶节点参与其中。参与签名过程的角色如下所示。

OBU_{A} 为原始签名人，m_{A} 为委任状。m_{A} 包含 OBU_{A} 的身份信息、门限值 t、代理签名者的身份、委任状有效期和签名范围的说明。

代理签名组 $\mathcal{P}_{\mathcal{B}}$ 由 n 个合法的代理签名人组成，即 $\mathcal{P}_{\mathcal{B}}=(OBU_{\mathrm{B}_1},OBU_{\mathrm{B}_2},\cdots,OBU_{\mathrm{B}_n})$，$ID_{\mathrm{B}_i}(i=1,2,\cdots,n)$ 为各代理签名人的身份标识。所有代理签名组成员的身份标识在系统初始化中已经被 OBU_{A} 获取。

实际代理签名组 $\mathcal{P}_{\mathcal{C}}$ 由 $\mathcal{P}_{\mathcal{B}}$ 中 t 个代理签名人组成，表示实际执行某次签名任务的 t 个代理签名组成员。$\mathcal{P}_{\mathcal{C}}=(OBU_{\mathrm{C}_1},OBU_{\mathrm{C}_2},\cdots,OBU_{\mathrm{C}_n})$，$ID_{\mathrm{C}_j}(j=1,2,\cdots,t)$ 是 $\mathcal{P}_{\mathcal{C}}$ 中各代理签名人的身份标识。

3.1　系统初始化

输入安全参数 k，KGC 执行如下操作。

1) 选择素数 q 阶加法循环群 $\mathbb{G}_1$ 和循环乘法群 $\mathbb{G}_2$，构造一个双线性映射 $e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$，并选择 $\mathbb{G}_1$ 的生成元 P。

2) 随机选择 $s\in Z_q^*$ 作为系统主密钥 msk，计算 $P_{\mathrm{pub}}=sP$ 为系统公钥。

3) 选取 3 个不同的单向 Hash 函数：$H_1,H_2:\{0,1\}^*\to Z_q^*$，$H_3:\{0,1\}^*\to\mathbb{G}_1$。

4) 公开系统参数 $params=(\mathbb{G}_1,\mathbb{G}_2,e,P,P_{\mathrm{pub}},H_1,H_2,H_3)$，并将系统主密钥 $msk=s$ 秘密保存。

3.2　生成用户私钥

在实际签名阶段，身份为 $ID_{\mathrm{C}_j}(j=1,2,\cdots,t)$ 的用户选择随机数 $\alpha_j\in Z_q^*$，将 $R_j=\alpha_jP$、$T_j=\alpha_jH_2(ID_{\mathrm{C}_j})$ 作为公钥公开，秘密值 α_j 作为私钥秘密保存。

3.3　生成代理密钥

代理密钥由 2 个部分组成：1) 原始签名人对代理签名人授权阶段产生的授权密钥；2) 代理人秘密共享阶段产生的共享密钥。

3.3.1　身份认证和授权密钥生成阶段

1) OBU_{A} 随机选择 $s_{\mathrm{A}}\in Z_q^*$，计算 $u_{\mathrm{A}}=s_{\mathrm{A}}P$ 并公开。

2) OBU_{A} 随机选择 $a_k\in Z_q^*(k=1,2,\cdots,t-1)$ 用来构造 $t-1$ 次多项式为

$$f(x)=s_{\mathrm{A}}+a_1x+\cdots+a_{t-1}x^{t-1} \tag{1}$$

计算 $A_k=a_kH_1(m_{\mathrm{A}})$，公开 A_k、$e(A_k,P),(k=1,2,\cdots,t-1)$。

3) 计算 $K_i=f(H_2(ID_{B_i}))H_1(m_A)(i=1,2,\cdots,n)$ 作为授权密钥，将 K_i 通过安全信道发送给对应的代理签名人 OBU_{B_i}。

4) 收到 K_i 后，每个代理签名人 OBU_{B_i} 计算 $e(K_i,P)=e(u_{\mathrm{A}},P)\prod_{i=1}^{t-1}e(A_k,p)H_2^i(ID_{\mathrm{B}_i})$ 是否成立，来验证 OBU_{A} 发送的代理子密钥是否有效。

3.3.2　共享密钥生成阶段

1) 每个代理签名人 $OBU_{\mathrm{B}_i}(i=1,2,\cdots,n)$ 任意选

取一个随机数 $s_j \in Z_q^*$，计算 $u_i = s_i P$ 并公开。当其中一个代理签名人 OBU_{B_i} 收到所有人发送的 u_i 后，计算 $U = \sum_{j=1}^{n} u_j$ 并公开。

2) OBU_{B_i} 随机选择 $b_{ik} \in Z_q^*(k = 1,2,\cdots,t-1)$ 构造 $t-1$ 次多项式为

$$g(x) = s_i + b_{i1}x + \cdots + b_{i(t-1)}x^{t-1} \tag{2}$$

计算 $B_{ik} = b_{ik}P$，公开 B_{ik}、$e(B_{ik}, P), (k = 1,2,\cdots, t-1)$。

3) OBU_{B_i} 计算 $S_i = g(H_2(ID_{\mathrm{B}_i}))P$，并通过秘密渠道发送给代理签名组 $\mathcal{P}_{\mathcal{B}}$ 中的其他成员。

4) 每个代理签名人 OBU_{B_i} 计算 $e(P, S_i) = e(P, u_i)\prod_{k=1}^{t-1} e(P, B_{ik})H_2^k(ID_{\mathrm{B}_i})$ 是否成立。如果成立，则 OBU_{B_i} 收到所有成员发送的 S_i 后，计算 $S = \sum_{i=1}^{n} S_i$，并将 S 作为代共享密钥存储起来。

5) 最后每个代理签名人将授权密钥 K_i 和共享密钥 S 一起作为代理密钥保存，$psk_i = (K_i, S)$。

3.4 门限代理签名

为了在委任状 m_{A} 下以原始签名人 OBU_{A} 的名义对消息 $m \in \{0,1\}^*$ 进行签名，每个实际代理签名人 $OBU_{\mathrm{C}_j}(j = 1,2,\cdots,t)$ 利用其用户私钥 α_j 和代理密钥 $psk_j = (K_j, S)$ 执行如下操作。

1) OBU_{C_j} 在收到实际代理签名组中所有成员的公钥 (R_j, T_j) 后，计算 $R = \sum_{j=1}^{n} R_j$，$T = \sum_{j=1}^{n} T_j$，$H = H_3(R+T)$，$E_j = \alpha_j sP$，$V_j = \alpha_j H + \lambda_j(K_j + S)H_1(m)$。其中，$\lambda_j = \prod_{OBU_{\mathrm{C}_i} \in \mathcal{P}_C, i \neq j} \frac{H_2(ID_{\mathrm{C}_i})}{H_2(ID_{\mathrm{C}_j}) - H_2(ID_{\mathrm{C}_i})}$。

2) 将 (V_j, E_j, R_j, T_j) 作为对消息 m 的部分门限代理签名发送给 $\mathcal{P}_C$ 中的代理群管理员 OBU_{M}。

3) 收到 $(V_j, E_j, R_j, T_j), j = 1,2,\cdots,t$ 后，OBU_{M} 通过验证 $e(E_j + T_j, P) = e(P_{\mathrm{pub}}, R_j)e(H_1(ID_{\mathrm{C}_j}), R_j)$ 来确认其诚实性。一旦所有部分门限代理签名的诚实性得到验证，则产生消息 m 的门限代理签名 $\sigma_{P_{\mathrm{A}}} = (U, V, R_1, R_2, \cdots, R_t, T_1, T_2, \cdots, T_t, H_2(t))$。其中，$V = \sum_{j=1}^{t} V_j$，$t$ 为当前时间。

3.5 门限代理签名验证

为了验证委任状 m_{A} 下对消息 m 签名的有效性，验证者检验 $e(P,V) = e(R,H)\ e(P, u_A H_1(m))e(P, UH_1(m))$ 是否成立，如果成立则接受该签名，否则拒绝。图 4 给出了该签名方案的形式化描述。

4 方案分析

4.1 正确性分析

定理 1 基于双重代理密钥的门限代理签名方案具有正确性。

证明 1) 授权验证（生成第一重代理密钥）的正确性

$$\begin{aligned} e(K_i, P) &= e\left(f\left(H_2(ID_{\mathrm{B}_i})\right)H_1(m_{\mathrm{A}}), P\right) \\ &= e\left(\sum_{i=0}^{t-1} a_i H_2^i(ID_{\mathrm{B}_i})H_1(m_{\mathrm{A}}), P\right) \\ &= e\left(s_{\mathrm{A}} + \sum_{i=1}^{t-1} A_i H_1(m_{\mathrm{A}}), P\right) \\ &= e(u_{\mathrm{A}}, P)\prod_{i=1}^{t-1} e(A_k, P)H_2^i(ID_{\mathrm{B}_i}) \end{aligned} \tag{3}$$

2) 秘密共享（生成第二重代理密钥）的正确性

$$\begin{aligned} e(P, S_i) &= e\left(P, g_i\left(H_2(ID_{\mathrm{B}_i})\right)P\right) \\ &= e\left(P, s_i + \sum_{k=1}^{t-1} b_{ik}H_2^k(ID_{B_i})P\right) \\ &= e(P, s_i P)e\left(P, \sum_{k=1}^{t-1} B_{ik}H_2^k(ID_{\mathrm{B}_i})\right) \\ &= e(P, u_i)\prod_{k=1}^{t-1} e(P, B_{ik})H_2^k(ID_{\mathrm{B}_i}) \end{aligned} \tag{4}$$

3) 签名验证的正确性

$$\begin{aligned} e(P,V) &= e\left(P, \sum_{j=1}^{t} a_j H + \lambda_j(K_j + S)H_1(m)\right) \\ &= e\left(P, \sum_{j=1}^{t} a_j H\right)e\left(P, \sum_{j=1}^{t} \lambda_j(K_j + S)H_1(m)\right) \\ &= e\left(P\sum_{j=1}^{t} a_j, H\right)e\left(P, \left(\sum_{j=1}^{t} \lambda_j \sum_{i=1}^{n} S_i\right)H_1(m)\right)\cdot \\ &\quad e\left(P, \sum_{j=1}^{t} \lambda_i f\left(H_2\left(ID_{\mathrm{B}_j}\right)\right)H_1\left(m_{\mathrm{A}}\right)H_1(m)\right) \\ &= e(R,H)e\left(P, s_{\mathrm{A}}H_1(m_{\mathrm{A}})H_1(m)\right)\cdot \\ &\quad e\left(P, \left(\sum_{j=1}^{t} \lambda_j \sum_{i=1}^{n} g_j(H_2(ID_{\mathrm{B}_1}))P\right)H_1(m)\right)\cdot \end{aligned}$$

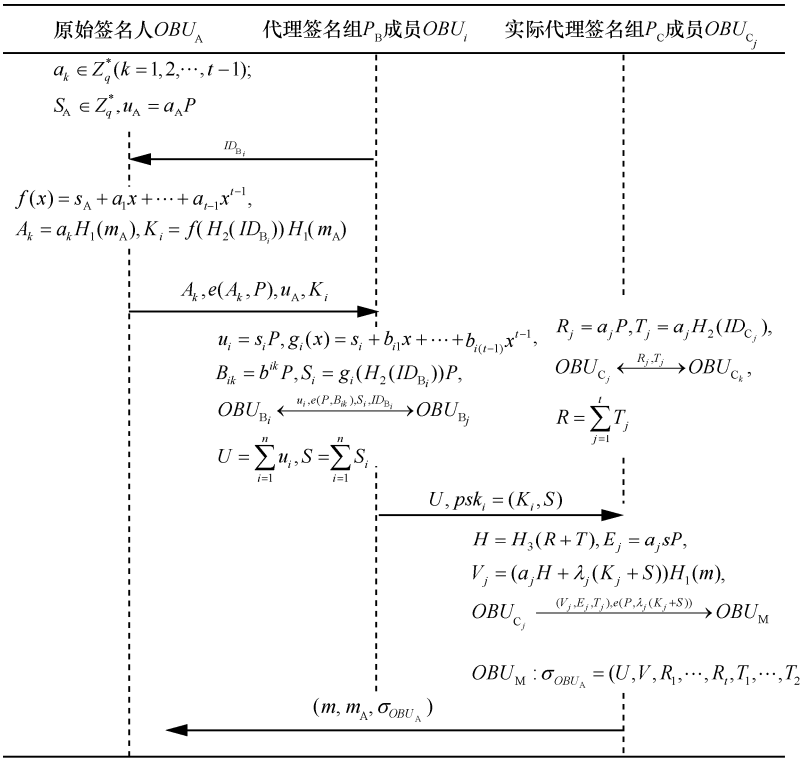


图 4　签名过程的形式化描述

$$e(R,H)e\left(P,u_{\mathrm{A}}H_1(m)\right)e\left(P,\left(\sum_{i=1}^{n}s_iP\right)H_1(m)\right)$$
$$=e(R,H)e\left(P,u_{\mathrm{A}}H_1(m)\right)e\left(P,UH_1(m)\right) \quad (5)$$

证毕。

4.2　安全性分析

假设攻击者可以获得其他 $t-1$ 个签名者的合谋攻击。一般地，如果一个数字签名体制在适应性选择消息攻击下能够抵抗存在性伪造，则该体制是安全的[26]。

与传统的门限代理签名方案不同的是，本文方案有三重密钥，即双重代理密钥和用户私钥。双重代理密钥指的是代理授权阶段产生的授权密钥 K_i 和秘密共享阶段产生的共享密钥 S。用户私钥指的是实际参与签名的成员 OBU_{C_j} 的私钥 $a_j(t \leqslant j \leqslant n)$。这种设计也更大程度地保证了签名的强不可伪造性、强可鉴别性、强不可否认性和防滥用性。

4.2.1　安全模型

在方案的安全模型中，攻击者 $\mathcal{A}_{\mathrm{adv}}$ 的具体攻击能力定义如下。

攻击者 $\mathcal{A}_{\mathrm{adv}}$ 没有系统主密钥，但是他可以进行 Hash 询问、身份授权询问、私钥提取询问和部分私钥询问、公钥询问、公钥替换询问，还可以进行加密和解密询问以及签名和验证询问[26]。

定义 1　存在性不可伪造[27]。称一个基于身份的门限代理签名方案在适应性选择消息攻击和适应性选择身份攻击下是 $(t,n,q_E,q_S,q_H,\varepsilon)$-安全的。如果不存在一个攻击者能够在 t 时间内至多产生 n 个子签名，进行 q_E 次私钥提取询问、q_S 次子代理签名询问和 q_{H} 次 Hash 询问后攻破它。

4.2.2　强不可伪造性

根据定义 1 可知，本文方案是存在性不可伪造的。

定理 2　在随机预言机模型下，如果一个敌手可以替换任意用户的长期公钥，但是不知道系统主密钥，那么由本文方案对于适应性选择消息攻击是存在性不可伪造的。

证明　假设存在多项式时间（PPT）算法 $\mathcal{A}_{\mathrm{adv}}$ 在多项式有界时间 t 内以一个不可忽略的概率 ε 成功伪造一个有效的签名，下面构造一个攻击者算法 $\mathcal{F}$ 解决离散对数问题（DLP）。设 $\mathcal{F}$ 是一个 DLP 挑战算法，以 $\mathcal{A}$ $ID_{\mathrm{B}_i}(i=1,2,\cdots,n)$ $_{\mathrm{adv}}$ 为子程序来求解 DLP：输入(xP, P)，输出x。$\mathcal{F}$ 发送系统参数给 $\mathcal{A}_{\mathrm{adv}}$，并维

持列表 L_f、L_g、L_1、L_2、L_3、L_D、L_K、L_S、L_{SIG} 分别用于跟踪算法 $\mathcal{A}_{\text{adv}}$ 对于 $f(x)$、$g(x)$、H_1、H_2、H_3、代理密钥提取、代理授权、用户私钥提取和代理签名生成的询问，初始化所有列表为空。用 q_f、q_g、q_1、q_2、q_3、q_D、q_k、q_s、q_{SIG} 来记录攻击者对 $f(x)$、$g(x)$、H_1、H_2、H_3、代理密钥、代理授权、用户私钥和签名生成的询问次数。攻击者对 $\mathcal{A}_{\text{adv}}$ 最多询问次数均为多项式有限次。

$\mathcal{F}$ 运行 Setup 算法，定义系统公钥 $Q=dP$，生成系统参数 $params=(\mathbb{G}_1,\mathbb{G}_2,e,P,P_{\text{pub}},H_1,H_2,H_3)$。$\mathcal{F}$ 随机选取 $ID_j=ID^*(1\leqslant j\leqslant q_i)$，$i$ 是 $\mathcal{A}_{\text{adv}}$ 访问 H_i 预言机的最大次数，然后把 *params* 和 ID^* 发送给 $\mathcal{A}_{\text{adv}}$，并秘密保存 d。

$\mathcal{A}_{\text{adv}}$ 适应性。当执行多项式数量级有界次数下的如下询问。

1) H_2-询问。当 $\mathcal{F}$ 关于 $H_2(ID)$ 询问时，若 $ID=ID^*$，则 $\mathcal{F}$ 随机选取 $h^*\in Z_q^*$，返回 h^*；否则返回 $h_m(1\leqslant m\leqslant q_2)$。最后将 (ID,h^*) 或 (ID,h_m) 添加到列表 L_2 中。

2) $f(x),g(x)$-询问。对于 $\mathcal{F}$ 关于 $f(H_2(ID))$ 或 $g(H_2(ID))$ 的询问，查询表 L_2 得到 ID 对应的值，若 $ID=ID^*$，则 $\mathcal{F}$ 随机选取 $f^*\in Z_q^*(g^*\in Z_q^*)$，返回 $f^*(g^*)$。否则返回 $f_m(g_m)(1\leqslant m\leqslant q_f(q_g))$。最后，将 (ID,h,f) 或 (ID,h,g) 记录到表 L_f 或 L_g，并输出 f 或 g 给 $\mathcal{A}_{\text{adv}}$。

3) H_1,H_3-询问。对于 $\mathcal{F}$ 关于 $H_1(m)$ 或 $H_3(m)$ 的询问，预言机随机选取整数 $n(1\leqslant n\leqslant q_1,q_3)$。如果表项中有 (m,h)，则 $\mathcal{F}$ 将 h 返回给 $\mathcal{A}_{\text{adv}}$ 作为 H_1 或 H_3 的散列值；否则，认为 $\mathcal{A}_{\text{adv}}$ 没有做过关于 H_1 或 H_3 的询问。如果 $i=n$，令 $h=eP$；否则 $i\neq n$，$\mathcal{F}$ 随机选取 $e_1\in Z_q^*$，令 $h=e_1P$。将 (m,h,e_1) 添加到列表 L_1 或 L_3 中，输出 h 给 $\mathcal{A}_{\text{adv}}$。

4) 授权询问。对于 $\mathcal{F}$ 关于 ID 授权的询问，这里考虑的是 $\mathcal{A}_{\text{adv}}$ 以代理人的身份询问的情形（假设已经做过关于 ID 的 $f(x)$ 询问和 H_2 询问，否则先执行 $f(x)$ 和 H_2 询问）。$\mathcal{F}$ 从列表 L_f 中找出 (ID,h_2,f)，如果 $ID=ID_m$，$\mathcal{F}$ 宣告失败，算法终止。否则 $\mathcal{F}$ 计算 $K=fh_1$，将 (ID,K) 记录到列表 L_D，输出 K 给 $\mathcal{A}_{\text{adv}}$ 作为授权结果。

5) 代理密钥询问。对于 $\mathcal{F}$ 关于 ID 的代理密钥询问（同样假设已经做过关于 ID 的 $g(x)$、H_2 和授权询问，否则先执行 $g(x)$、H_2 和授权询问）。$\mathcal{F}$ 从列表中找出 (ID,h_2,g) 和 (ID,K)，如果 $ID=ID_m$，$\mathcal{F}$ 宣告失败，算法终止。否则 $\mathcal{F}$ 计算 $psk=K+gP$，将 (ID,psk) 记录到列表 L_k，输出 H 给 $\mathcal{A}_{\text{adv}}$ 作为代理密钥。

6) 公钥替换。若签名者身份为 ID，则 $\mathcal{A}_{\text{adv}}$ 可以任选一个新的公钥替换签名者的原公钥。

7) 用户私钥询问。$\mathcal{A}_{\text{adv}}$ 提交关于 ID 的私钥询问，如果公钥已经被替换，则 $\mathcal{F}$ 输出 $\perp$ 作为答复。否则，假设已经做过关于 ID 的 H_2 询问，先执行 H_2 询问。随机选取 $x_{ID}\in Z_q^*$，查询列表 L_2 得到 (ID,h_2)，$\mathcal{F}$ 计算 $R=x_{ID}P$、$T=x_{ID}h_2$，将 (ID,R,T,x_{ID}) 记录到 L_S，输出 (R,T) 给 $\mathcal{A}_{\text{adv}}$，秘密存储 x_{ID}。

8) 代理子签名生成询问。$\mathcal{A}_{\text{adv}}$ 提交关于 (ID,m,m_{A}) 的代理子签名询问，首先查询 L_1、L_2，得到 (ID,h_2)、(m,h_1)，随机选取 $psk,v,h_3,\alpha,\lambda\in Z_q^*$，查询 L_3，使 $h_1H_3(aP+ah_2)=v-\lambda psk$。令 $R=\alpha P$、$T=\alpha h$，查询 L_s，若 (R,T) 存在，则 $\mathcal{F}$ 失败并终止。否则将 (m,m_A,v) 发送给 $\mathcal{A}_{\text{adv}}$。并将 (ID,R,T) 添加至表 L_s 中。

9) 伪造。若上述过程算法没有终止，则可认为 $\mathcal{A}_{\text{adv}}$ 在没有做过代理子密钥询问、用户私钥询问和代理子签名询问的条件下，以一个不可忽略的概率 ε 完成了对一个消息 m 的签名 (m,m_A,v')。

根据分叉引理[28]，通过对 $\mathcal{A}_{\text{adv}}$ 的散列重放，存在一个有效的算法使 $\mathcal{A}_{\text{adv}}$ 可以获得对委任状 m_{A} 下消息 m 的 2 个不同的有效签名 (m,m_{A},v_1')、(m,m_{A},v_2')。从而可以得出

$$\begin{cases} v_1'=(aH_1^*+\lambda_1^*(K_1^*+S))H_1(m) \\ v_2'=(aH_2^*+\lambda_2^*(K_2^*+S))H_2(m) \end{cases} \tag{6}$$

根据式(6)可以解得 $\alpha=\dfrac{\dfrac{v_1'-v_2'}{H_1(m)}-\lambda_1^*(K_1^*+S)+\lambda_2^*(K_2^*+S)}{H_1^*-H_2^*}$，算法 $\mathcal{F}$ 的运行时间 $t'\approx\dfrac{(o(q_{\text{SIG}}\tau_{\text{adv}})+(q_f+q_g+q_1+q_2+q_3)\tau)+t}{\varepsilon}$。其中，$\tau$ 为回答一个散列提问或 $f(x),g(x)$-询问的时间。

综上，结合这 2 个有效的子代理签名，可以认

为算法 $\mathcal{F}$ 在多项式时间内以一个不可忽略的概率解决了离散对数问题。而 DLP 是一个公认的困难问题，从而反证出本文所提出的基于双重代理密钥的门限代理签名方案对自适应选择和身份攻击是存在性不可伪造的。证毕。

事实上，双重代理密钥的设计使仅凭原始签名人 OBU_{A} 或代理签名组 $\mathcal{P}_{\mathcal{B}}$ 的任意成员都无法获得全部代理密钥，所以任意一方被感染都无法伪造有效签名。另外，门限代理签名的思想保证了任意少于 t 个合法代理签名人的组合都无法重构出秘密值，从而保证了它们无法通过验证。这就是本文方案的强不可伪造性。

4.2.3　强可鉴别性

考虑到海洋通信环境的复杂多变性，RAS 和 AP 并没有被强制参与签名过程。但是任意合法的 OBU_{B_i} 节点和原始签名人 OBU_{A} 将可以通过委任状 m_{A} 来确认委托双方的身份，并且产生双重代理密钥也都需要身份验证，这保证了本文方案的强可鉴别性。

4.2.4　强不可否认性

在生成双重代理密钥时，用到了 OBU_{A} 和 OBU_{B_i} 的身份信息，这可以保证代理签名组 $\mathcal{P}_{\mathcal{B}}$ 的任意成员都可以验证实际执行签名成员 OBU_{C_j} 的身份。当某个代理签名人 OBU_{C_j} 产生了一个合法的子签名 (V_j,E_j,R_j,T_j) 时，这个子签名中就包含了 (V_j,E_j,R_j,T_j) 的身份信息 ID_{C_j}。并且只有这些合法的签名人才能重构出签名密钥，所以他们无法对该签名抵赖。

4.2.5　防滥用性

原始签名人 OBU_{A} 的委任状 m_{A} 包含了代理签名组 $\mathcal{P}_{\mathcal{B}}$ 所有成员的身份信息，包含他们的身份标识、签名权限、有效期限。这保证了任意一个合法代理签名人都只能在合法的时间段内对权限内的消息签名。

4.3　效率分析

4.3.1　计算复杂度分析

表 1 给出了本文方案与其他典型的门限代理签名方案的计算复杂度比较。令 T_{exp} 表示循环群上的一次乘方运算，T_{mul} 表示循环群上的一次点乘运算，T_{mtp} 表示一次 Map2Point 散列运算，T_{par} 表示一次双线性映射运算。文献[20-22]的 T_{exp}、T_{mul}、T_{mtp} 和 T_{par} 的运行时间分别为 0.46 ms、0.6 ms、3.9 ms 和 4.9 ms。用 $|m_{\mathrm{A}}|$ 表示委任状的长度，$|ID|$ 表示用户 ID 的长度，$|m|$ 表示签名消息的长度，t 表示实际代理签名人的数量，n 表示代理签名组所有成员的数量。称上述变量为衡量方案计算复杂度的系统参数。从表 1 不难看出，除本文方案外，其他 3 种门限代理签名方案的计算复杂度分别与委任状 m_{A} 的长度和用户 ID 的长度、参与门限签名的签名人个数以及签名消息 m 的长度有关。这是因为本文方案将 m_{A}、ID 和 m 通过 Map2Point 散列函数映射到 Z_q^* 上，消除了消息长度对计算复杂度的影响，同时增强了安全性。但这种做法在消息长度较短的应用场景下会增加 Map2Point 散列运算的时间。另外，本文方案在验证签名时的计算复杂度相对于文献[20]的方案有较明显的优势；对于文献[18-19]的方案，虽然本文方案要多花费一次计算双线性映射的时间，但是上述 2 种方案的计算复杂度较容易受到系统参数（如消息长度和代理签名人个数等）的影响，当文献[18-19]中方案的系统参数变化时，方案验证签名的计算复杂度会随之波动，而本文方案验证签名的计算复杂度较为稳定。不可否认的是，当系统参数的取值较小时，文献[18-19]方案的计算复杂度要优于本文方案。

4.3.2　通信复杂度分析

记 $|Z_q^*|$ 为 Z_q^* 中元素的长度，记 $|\mathbb{G}_1|$ 为 $\mathbb{G}_1$ 中元素的长度，记 $|\mathbb{G}_2|$ 为 $\mathbb{G}_2$ 中元素的长度，表 2 给出了本文方案与其他典型的门限代理签名方案的通

表 1　　**计算复杂度比较**

方案	生成签名	验证签名
本文方案	$2T_{\mathrm{mtp}}+4T_{\mathrm{mul}}$	$7T_{\mathrm{par}}$
文献[18]的方案	$(\|m_{\mathrm{A}}\|+5(t-1))T_{\mathrm{mul}}+2\ T_{\mathrm{exp}}$	$6T_{\mathrm{par}}+(t+4)T_{\mathrm{exp}}+2(\|m_{\mathrm{A}}\|+\|\mathrm{ID}\|+t+10)T_{\mathrm{mul}}$
文献[19]的方案	$3(n+1)T_{\mathrm{mul}}+T_{\mathrm{mtp}}$	$6T_{\mathrm{par}}+4T_{\mathrm{exp}}+2T_{\mathrm{mtp}}+2n^2T_{\mathrm{mul}}$
文献[20]的方案	$2\|m\|T_{\mathrm{mul}}+4T_{\mathrm{exp}}$	$7T_{\mathrm{par}}+2\|m\|T_{\mathrm{mul}}$

信复杂度比较。

表 2　　通信复杂度比较

方案	签名长度/B
本文方案	$4t\|Z_q^*\|$
文献[18]的方案	$4\|\mathbb{G}_1\|+(t-1)\|\mathbb{G}_2\|$
文献[19]的方案	$t(\|Z_q^*\|+2\|\mathbb{G}_1\|)$
文献[20]的方案	$3t\|\mathbb{G}_1\|$

从表 2 不难看出，以子签名长度作为方案通信复杂度衡量的标准时，只有在$Z_q^* \leqslant \frac{3}{4}\mathbb{G}_1$、$Z_q^* \leqslant \frac{3}{4}\mathbb{G}_2$的前提下，本文方案的通信复杂度才会比其他 3 种门限代理签名方案具有优势。原因在于为了更好地保证恶劣环境条件下船舶自组网的安全通信，本文为门限代理签名方案设计了双重代理密钥，而两重加密过程相比单次加密过程增加了消息长度。事实上，通过对签名方案初始化程序的限制，在实际应用场景中上述条件是容易满足的，即本文提出的船舶自组网门限代理签名方案在一定条件下相比其他门限代理签名方案具有一定的优势。

5　结束语

本文针对船舶自组网的安全通信问题，结合船舶自组网的特点，提出了一种基于双重代理密钥的门限签名方案。在该方案中，船舶节点可以在不依赖固定基础设施的情况下保障通信安全。分析表明，本文方案在船舶自组网特定的应用环境下具有较低的计算开销和通信开销，并且在保证方案正确性的前提下可以满足强代理签名的性质。通过随机预言模型的理论分析可以得出，该方案也是抗合谋攻击的。

参考文献：

[1] SU X, HUI B, CHANG K H. Multi-hop clock synchronization based on robust reference node selection for ship ad-hoc network[J]. Journal of Communications & Networks, 2016, 18(1):65-74.

[2] PAPI F, TARCIH D, VESPE M, et al. Radiolocation and tracking of automatic identification system signals for maritime situational awareness[J]. Radar Sonar & Navigation Iet, 2015, 9(5):568-580.

[3] ZHOU M ,VEEN A J V D. Blind beamforming techniques for automatic identification system using GSVD and tracking[C]// IEEE International Conference on Acoustics, Speech and Signal Processing. 2014: 3012-3016.

[4] YANG J, CHENG Y, CHEN L. The detection probability modeling and application study of satellite-based AIS system[C]// IEEE Information Technology and Artificial Intelligence Conference. 2015: 28-33.

[5] ZHOU M T, HOANG V D, HARADA H, et al. TRITON: high-speed maritime wireless mesh network[J]. IEEE Wireless Communications, 2013, 20(5): 134-142.

[6] YANG T, ZHENG Z, LIANG H, et al. Green energy and content-aware data transmissions in maritime wireless communication networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(2): 751-762.

[7] YANG T, LIANG H, CHENG N, et al. Efficient scheduling for video transmissions in maritime wireless communication networks[J]. IEEE Transactions on Vehicular Technology, 2015, 64(9):4215-4229.

[8] HUA C, SHEN Z, LU J. High-efficiency sea-water monopole antenna for maritime wireless communications[J]. IEEE Transactions on Antennas & Propagation, 2014, 62(12): 5968-5973.

[9] LANDY J C, KOMAROV A S, BARBER D G, et al. Numerical and experimental evaluation of terrestrial LiDAR for parameterizing centimeter-scale sea ice surface roughness[J]. IEEE Transactions on Geoscience and Remote Sensing, 2015, 53(9): 4887-4898.

[10] 吴黎兵, 谢永, 张宇波. 面向车联网高效安全的消息认证方案[J]. 通信学报，2016, 37(11):1-10.
WU L B, XIE Y, ZHANG Y B. Efficient and secure message authentication scheme for VANET [J].Journal on Communications, 2016, 37(11):1-10.

[11] KIM Y B, KIM J H, WANG Y P, et al. Application scenarios of nautical ad-hoc network for maritime communications[C]// IEEE Oceans. 2009: 1-4.

[12] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures: delegation of the power to sign messages[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1996, 79(9): 1338-1354.

[13] ZHANG F, KIM K. Efficient ID-based blind signature and proxy signature from bilinear pairings[C]//ACISP'2003, LNCS 2727. 2003: 312-323.

[14] QIAN H, CAO Z, XUE Q. Efficient pairing-based threshold proxy signature scheme with known signers[M]. IOS Press, 2005.

[15] WU W, MU Y, SUSLIO W, et al. Identity-based proxy signature from pairings[C]//International Conference on Autonomic and Trusted Computing. 2007:22-31.

[16] LIU J, HUANG S. Identity-based threshold proxy signature from bilinear pairings[M]. IOS Press, 2010.

[17] YANG T, XIONG H, HU J, et al. A traceable certificateless threshold proxy signature scheme from bilinear pairings[C]// Asia-Pacific Web Conference on Web Technologies and Applications. 2011:376-381.

[18] 于义科, 郑雪峰. 标准模型下基于身份的高效动态门限代理签名方案[J]. 通信学报, 2011, 32(8):55-63.
YU Y K, ZHENG X F. ID-based efficient and proactive threshold proxy signature in the standard model[J]. Journal on Communications,

2011, 32(8):55-63.

[19] MENG X, LI Y. A novel verifiable threshold signature scheme based on bilinear pairing in mobile ad hoc network[C]// International Conference on Information and Automation. 2012:361-366.

[20] QIN H, ZHU X, DAI Y. Provably secure identity-based threshold signature on access structure[M]. 2014.

[21] SHAO J, LIN X, LU R, et al. A threshold anonymous authentication protocol for VANETs[J]. IEEE Transactions on Vehicular Technology, 2016, 65(3): 1711-1720.

[22] YEH L Y, LIN Y C. A proxy-based authentication and billing scheme with incentive-aware multihop forwarding for vehicular networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2014, 15(4): 1607-1621.

[23] SHUM K, WEI V K. A strong proxy signature scheme with proxy signer privacy protection[C]// Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. 2002: 55-56.

[24] KENNEY J B. Dedicated short-range communications (DSRC) standards in the united states[J]. Proceedings of the IEEE, 2011, 99(7): 1162-1182.

[25] HUI B, JEON K H, CHANG K H, et al. Design of radio transmission technologies for VHF band ship ad-hoc network[C]// IEEE International Conference on ICT Convergence.2011: 626-629.

[26] 牛淑芬, 牛灵, 王彩芬, 等. 标准模型下可证明安全的无证书广义签密 [J]. 通信学报, 2017, 38(4):35-45.
NIU S F, NIU L, WANG C F, et al. Certificateless generalized signcryption scheme in the standard model[J]. Journal on Communications, 2017, 38(4):35-45.

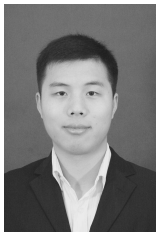
[27] 张华, 温巧燕, 金正平. 可证明安全算法与协议[M]. 北京: 科学出版社, 2012.
ZHANG H, WEN Q Y, JIN Z P. Provable security algorithm and protocol[M]. Beijing: Science Press, 2012.

[28] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报, 2005, 16(10):1743-1756.
FENG D G. Research on theory and approach of provable security[J]. Journal of Software, 2005, 16(10): 1743-1756.

[作者简介]

徐明（1977−），男，安徽马鞍山人，博士，上海海事大学副教授，主要研究方向为无线通信网络、网络空间安全等。

李旭如（1995−），女，安徽宣城人，上海海事大学硕士生，主要研究方向为无线通信网络、网络空间安全等。



刘朝斌（1985−），男，河南封丘人，复旦大学博士生，主要研究方向为隐私保护、计算机网络安全等。

马尧（1986−），男，河南许昌人，博士，中国通用技术研究院工程师，主要研究方向为大数据技术、信息安全等。