

面向边缘计算的隐私保护密钥分配协议

沈剑, 周天祺, 王晨, 杨惠杰

(南京信息工程大学江苏省网络监控工程中心, 江苏 南京 210044)

摘要: 针对边缘计算多应用场景下的隐私保护问题, 提出两种基于策略的密钥分配协议, 所提出的协议基于约束伪随机函数的概念分别实现了轻量高效和灵活细粒度的策略选择。具体来说, 基于 GGM 伪随机数生成器, 构建前缀谓词策略的密钥分配协议, 该协议可有效支持轻量高效的密钥分配, 适用于单一网络环境下设备资源受限的应用场景。在此基础上, 基于多线性对, 构建位固定谓词策略的密钥分配协议, 该协议可支持灵活细粒度的策略选择, 适用于异构网络动态灵活的多设备场景。最后, 通过形式化证明分析所提出协议的安全性。

关键词: 边缘计算; 隐私保护; 约束伪随机函数; 密钥分配

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021010

Privacy protection key distribution protocol for edge computing

SHEN Jian, ZHOU Tianqi, WANG Chen, YANG Huijie

Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing 210044, China

Abstract: Aiming at the privacy protection problem in the multi-application scenarios of edge computing, two policy-based key distribution protocols were proposed. The proposed protocols are based on the concept of constrained pseudo-random functions to achieve efficient and flexible policy selection. Specifically, based on the GGM pseudo-random number generator, the key distribution protocol with a prefix-predicate is constructed, which can effectively support lightweight and efficient key distribution. Moreover, based on the multilinear pairing, the key distribution protocol with a bit-fixed predicate is constructed, which can support flexible and fine-grained policy selection. Finally, the security of the proposed protocols is analyzed by formalized proof analysis.

收稿日期: 2020-12-14; 修回日期: 2021-01-03

通信作者: 沈剑, s_shenjian@126.com

基金项目: 国家自然科学基金(U1836115, 61672295, 61922045, 61672290, 61877034); 江苏省自然科学基金(BK20181408); 鹏城实验室网络空间安全研究中心(PCL2018KP004); 2020年江苏省研究生科研创新计划(KYCX20-0936)

Foundation Items: The National Natural Science Foundation of China (U1836115, 61672295, 61922045, 61672290, 61877034), The Natural Science Foundation of Jiangsu Province (BK20181408), Cyberspace Security Research Center, Peng Cheng Laboratory Project of Guangdong Province (PCL2018KP004), 2020 Research Innovation Program for Postgraduates of Jiangsu Province (KYCX20-0936)

论文引用格式: 沈剑, 周天祺, 王晨, 等. 面向边缘计算的隐私保护密钥分配协议[J]. 网络与信息安全学报, 2021, 7(1): 93-100.

SHEN J, ZHOU T Q, WANG C, et al. Privacy protection key distribution protocol for edge computing[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 93-100.

bution protocol with a bit fixing predicate is constructed. This protocol can support flexible and fine-grained strategy selection and is suitable for dynamic and flexible multi-device scenarios in heterogeneous networks. Finally, the security proof of the proposed protocols is presented.

Keywords: edge computing, privacy protection, constrained pseudorandom function, key distribution

1 引言

随着物联网的发展和广泛应用,边缘计算以其低时延、高可靠、海量连接、异构汇聚等优点受到越来越多的关注。作为物联网的关键技术,物联网基础设施的建设将引起边缘计算的进一步发展。据统计,物联网连接数量在2018年开始爆发式增长。2010—2018年全球物联网设备数量高速增长,复合增长率达20.9%。预测2025年全球物联网设备将达到252亿个^[1]。由此可见,边缘计算在未来几年内将迎来新的发展机遇,与此同时,将迎来新的挑战^[2]。

边缘计算处理包括智能家居、智能驾驶、智慧安防等多种场景下的设备接入并需要为接入设备的安全通信提供保障,这就要求认证、签名、加密等密码技术的合理部署。在各种密码技术中,如何在公开的不安全的网络环境下产生通信双方共享的密钥是各种密码技术实施的关键。与此同时,随着人们隐私保护^[3]意识的增强,边缘计算不但需要提供高可靠的安全访问,更需要在异构网络中为不同的应用场景提供灵活动态的隐私保护机制。共享密钥作为各种密码技术实施的前提,密钥分配^[4]过程中的隐私保护将成为边缘计算环境下隐私保护的第一道关卡。

目前,密钥分配协议往往针对付费电视、视频会议、云存储等单一环境,无法直接应用于边缘计算动态多变的多场景环境。此外,现有的密钥分配协议大多基于身份基加密、认证、签名等密码体制,无法保障分配过程中的用户隐私。

1.1 相关工作

针对车联网中的密钥管理问题,文献[5]基于公钥基础设施提出了一种匿名密钥管理方案。然而,随着接入节点的增多和动态变化,证书的管理将变得低效而复杂。文献[6]提出了一种基于特殊组合结构的密钥协商方案,该方案可以为云环境下多用户数据共享安全提供保障,并且使用的对称平衡不完全区组设计结构可以极大地降低协

商的通信开销。在此基础上,文献[7]提出了支撑匿名的群组密钥方案,能够保证云环境下的用户隐私安全。借助分布式并行计算,文献[8]提出了一种支持动态操作的密钥协商协议,能够保证车联网环境下多用户的安全交互。虽然上述协议实现了公开网络下多用户的密钥生成,然而,边缘计算中的付费应用或者访问控制机制往往需要多设备的集中管理或者分层结构模式。由此,密钥分配协议更适用于边缘计算中的集中管理结构。文献[9]提出了一种车联网中安全即时通信的密钥分配方案,然而,该协议仅能支持两方进行密钥分配。此外,密钥分配过程需要安全的通信信道。文献[10]提出了一种基于强化学习的群密钥分配管理技术,该协议能够支持群组用户的密钥分配,降低加解密时延。然而,缺少形式化的安全性分析和证明。

密钥作为边缘计算中安全传输、身份认证^[11-12]以及数据加密的基础,为边缘计算的安全提供了有力的保障。同时,密钥分配过程中的隐私保护问题是实现边缘计算本地安全隐私保护的重要一环。基于策略选择的非交互式密钥分配是隐私保护的有效实现方案。具体来说,基于策略选择的非交互式密钥分配指的是:由复杂策略标识的一组用户可以非交互式地建立秘密组密钥,该密钥可用于组成员之间的安全通信。

1.2 本文工作

本文针对边缘计算异构网络中的隐私保护问题,提出了两种基于策略的密钥分配协议,所提协议可以实现轻量高效和灵活细粒度的密钥分配。本文的贡献总结如下。

(1) 设计了基于约束伪随机函数的策略选择。针对边缘计算中的本地安全隐私保护问题,本文基于约束伪随机函数^[13]的概念实现了密钥分配的策略选择。在此基础上,分别实现了边缘计算多应用场景的轻量高效和灵活细粒度的策略选择,为边缘计算多场景下的隐私保护提供技术支撑。

(2) 提出了基于前缀谓词 (prefix predicate) 策略的密钥分配协议。针对单一网络环境下设备资源受限的场景中的密钥分配问题, 本文提出了一种基于前缀谓词策略的密钥分配协议, 该协议可以支持资源受限设备进行高效轻量的密钥分配。具体来说, 基于 GGM 伪随机数生成器^[14], 构建前缀谓词约束的伪随机函数, 并利用 GGM 的高效构建以及前缀约束的简单易实现的性质, 有效支持边缘资源受限设备的高效密钥分配。

(3) 提出了基于位固定谓词 (bit fixing predicate) 策略的密钥分配协议。针对异构网络动态灵活的多设备场景中的密钥分配问题, 本文提出了一种基于位固定谓词策略的密钥分配协议, 该协议可以支持动态灵活的策略选择。具体来说, 基于多线性对, 构建位固定谓词约束的伪随机函数, 并利用多线性对分布计算的优点, 巧妙地设计出一种支持动态灵活策略选择的密钥分配协议, 有效支持边缘动态设备基于策略选择的密钥分配。

(4) 形式化安全性证明。形式化定义密钥协商安全模型, 模拟现实环境中攻击者所具备的能力。在此基础上, 基于 K-MDDH 假设, 在 ROM 模型下分析并证明所提出协议的安全性。

2 预备知识

本节介绍协议相关的密码学预备知识。

2.1 多线性对

多线性对^[15]: 对于一个群组生成元 $\mathcal{G}$, 给定安全参数 λ 以及一个描述层级的正整数 κ , $\mathcal{G}(1^\lambda, \kappa)$ 将输出一系列循环群 $G = (G_1, G_2, G_3, \dots, G_\kappa)$, 每个群都有一个大素数的阶 $p > 2^\lambda$ 。此外, 令 g_i 为描述每个群的正规化生成元。假设存在一系列的双线性映射 $e_{i,j}: G_i \times G_j \rightarrow G_{i+j} | i, j \geq 1; i+j \leq \kappa$ 且该 $e_{i,j}$ 映射满足如下关系。

$$e_{i,j}(g_i^a, g_j^b) = g_{i+j}^{ab} : a, b \in \mathbb{Z}_p^*$$

定义 1 多线性对决定性 Diffie-Hellman (K-MDDH) 假设^[16]。给定多线性对 $\mathcal{G}(1^\lambda, \kappa)$ 的公开参数, 攻击者 $\mathcal{A}$ 随机选择 $\kappa+1$ 个随机元素 $c_1, c_2, c_3, \dots, c_{\kappa+1} \in \mathbb{Z}_p^*$, 定义攻击者 $\mathcal{A}$ 解决 K-MDDH

的优势为式(1)。

$$\text{Adv}_{\mathcal{A}}^{\text{K-MDDH}} = \Pr[|\text{Exp}_0 = 1| - |\text{Exp}_1 = 1|] \quad (1)$$

其中, Exp_0 表示事件, 即 $\mathcal{A}$ 在已知 $g, g^{c_1}, g^{c_2}, g^{c_3}, \dots,$

$g^{c_{\kappa+1}}, g_1 = g$ 的情况下得到 $g_{\kappa}^{\prod_{i=1}^{\kappa+1} c_i} \in G_{\kappa}$; Exp_1 表示事件, 即 $\mathcal{A}$ 在已知 $g, g^{c_1}, g^{c_2}, g^{c_3}, \dots, g^{c_{\kappa+1}}$ 的情况下得到 G_{κ} 中随机选取的元素 r 。实验后, 攻击者输出 0, 代表收到的是一个随机值, 输出为 1, 代表收到的 $g_{\kappa}^{\prod_{i=1}^{\kappa+1} c_i} \in G_{\kappa}$ 。在 K-MDDH 假设下, 攻击者 $\mathcal{A}$ 的优势 $\text{Adv}_{\mathcal{A}}^{\text{K-MDDH}}$ 是可忽略的。

2.2 伪随机函数

定义 2 伪随机函数 $F: \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$ 是一个可以在多项式时间内确定性计算的函数。给定密钥空间中的一个密钥 $k \in \mathcal{K}$, 函数 $F(k, \cdot)$ 可以有效地计算输入空间中任意一点 $x \in \mathcal{X}$ 的伪随机函数值 $F(k, x)$ ^[14]。伪随机函数的安全性要求其输出与一个同等长度的随机数是不可区分的。

2.3 前缀谓词

定义 3 给定 n 位向量 $\mathbf{v} \in \{0, 1\}^{n-l}$, 前缀谓词 $\mathcal{P}_{\mathbf{v}}^P: \{0, 1\}^n \rightarrow \{0, 1\}$ 是一个输出为 0 或 1 的函数, 式(2)定义了 $\mathcal{P}_{\mathbf{v}}^P$ 的具体计算方式。

$$\mathcal{P}_{\mathbf{v}}^P(x) = 1 \Leftrightarrow v_i = x_i \text{ for } (i \leq l), v_i = ? \text{ for } (l < i \leq n), l \in [n] \quad (2)$$

即给定输入 x 谓词, $\mathcal{P}_{\mathbf{v}}^P$ 输出 1 当且仅当输入的前 l 位与向量 $\mathbf{v}$ 的前 l 位完全匹配, 其中 “?” 表示在谓词判定中该位是非约束位, 其上的值为 0 或 1 都不会影响输出结果。

2.4 位固定谓词

定义 4 给定 n 位向量 $\mathbf{v} \in \{0, 1, ?\}^n$, 位固定谓词 $\mathcal{P}_{\mathbf{v}}^{BF}: \{0, 1\}^n \rightarrow \{0, 1\}$ 是一个输出为 0 或 1 的函数, 式(3)定义了 $\mathcal{P}_{\mathbf{v}}^{BF}$ 的具体计算方式。

$$\mathcal{P}_{\mathbf{v}}^{BF}(x) = 1 \Leftrightarrow v_i = x_i \text{ or } v_i = ? \text{ for } (1 \leq i \leq n) \quad (3)$$

即给定输入 x 谓词 $\mathcal{P}_{\mathbf{v}}^{BF}$ 输出 1 当且仅当输入与其每一个对应的非约束位 (即非 “?” 所在的位) 完全匹配。

2.5 基于策略的密钥分配

定义 5 对于一个包含 n 个用户的密钥分配系统, 每个用户都被一个属性向量 att_i 唯一标识。

基于策略的密钥分配使一个具备属性 att_i 的用户可以计算共享密钥当且仅当用户的属性集合对于谓词 $\mathcal{P}$ 满足 $\mathcal{P}(att_i)=1$ 。

为方便读者阅读,表 1 给出了本文常见符号及其对应说明。

表 1 符号说明
Table 1 Notations

符号	说明
λ	系统安全参数
msk	主私钥
sk_i	用户私钥
K_i	会话密钥
att_i	用户属性
PRF	伪随机函数

3 系统模型和安全模型

3.1 系统模型

本文所设计的协议系统模型如图 1 所示。针对边缘计算中的不同需求设计基于前缀谓词策略的密钥分配协议以及基于位固定谓词策略的密钥分配协议。其中,基于前缀谓词策略的密钥分配协议具备轻量高效的特点,适用于智慧气象采集节点以及智能家居中的不同设备;基于前缀谓词策略的密钥分配协议具备灵活动态的特点,可有效支撑智慧安防以及智能驾驶中接入设备动态多变的特点。协议的实体主要包括边缘设备、边缘层和云。其中,边缘设备主要由智慧气象、智能

家居、智慧安防、智能驾驶等传感器设备构成,设备间的安全通信或者共享需要密钥的支持;边缘层负责收集边缘设备的数据进行处理,边缘层与设备间的交互需要密钥保证安全;云负责存储和批量处理数据后向边缘设备进行反馈,云与边缘层的交互需要密钥对传输数据进行保护。

3.2 安全模型

本文所提出的密钥分配协议包括以下 3 个算法。

1) 初始化算法 $\text{Setup}(\lambda)$: 输入系统安全参数 λ , 返回系统参数 param 以及主私钥 msk 。

2) 私钥提取算法 $\text{Extract}(msk, att_i)$: 输入属性 att_i 和系统主私钥, 返回属性为 att_i 的私钥 sk_i 。其中, 私钥 sk_i 是属性为 att_i 的对应约束伪随机函数的约束密钥。

3) 共享密钥提取算法 $\text{Reveal}(att_i, sk_i)$: 输入属性 att_i 和约束密钥 sk_i , 返回属性为 att_i , 约束私钥为 sk_i 的用户的共享密钥 K_i 。其中, 共享密钥 K_i 为通过约束密钥 sk_i 计算的约束伪随机函数的函数值。

基于 Dupont 和 Enge^[17]以及 Paterson 和 Srinivasan^[18]的工作, 本文提出了一种改进的基于策略的非交互式密钥分配协议安全模型。在所提出的模型中, 攻击者 $\mathcal{A}$ 具备系统初始化、私钥提取、共享密钥提取的能力, 其详细描述如下。

1) 初始化算法 $\text{Setup}(\lambda)$: 输入系统安全参数 λ , 返回系统参数 param 、 msk 。

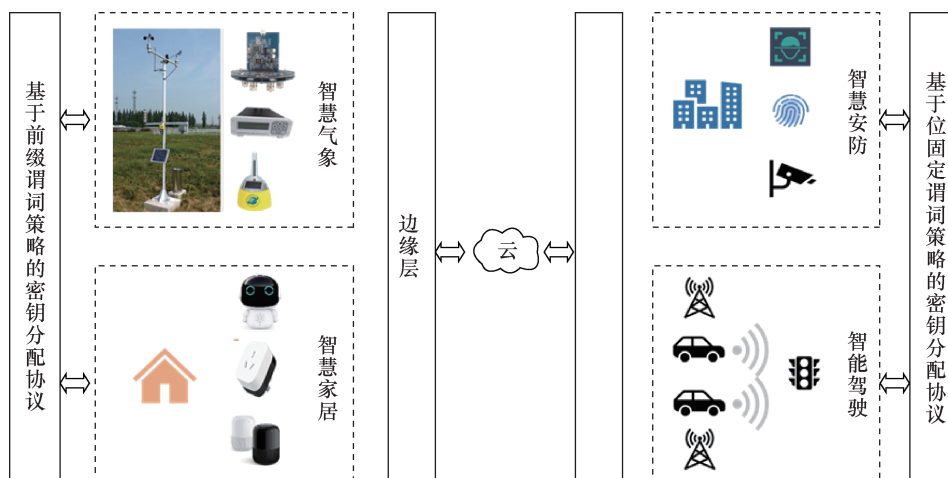


图 1 系统模型

Figure 1 The system model

2) 私钥提取询问 $\text{Extract}(\text{att}_i)$ ：返回属性为 att_i 的用户私钥 sk_i 。

3) 共享密钥提取询问 $\text{Reveal}(\text{att}_i)$ ：返回属性为 att_i 、私钥为 sk_i 的用户的共享密钥 $\mathcal{K}_i$ 。

4) 挑战算法 $\text{Test}(\text{att}_i)$ ：攻击者 $\mathcal{A}$ 在进行任意多次私钥提取询问和共享密钥提取询问后，选取一个欲挑战的属性 att_i （该属性没有进行私钥提取和共享密钥提取询问），挑战者 $\mathcal{C}$ 返回一个随机值或者属性 att_i 对应的共享密钥。攻击者 $\mathcal{A}$ 需要区分所获得的值是共享密钥还是随机值。

协议的安全性要求：攻击者 $\mathcal{A}$ 可进行任意多次 $\text{Extract}(\text{msk}, \text{att}_i)$ 询问，获得一系列属性 $A^{\text{Ext}} = \{\text{att}_i\}$ 所对应的私钥。此外，攻击者 $\mathcal{A}$ 可以询问任意不等于挑战属性 att_i 的属性 $\text{att}_j \neq \text{att}_i$ 所对应的共享密钥。协议的安全性要求为，攻击者 $\mathcal{A}$ 在进行上述询问后，在挑战阶段，对于任意挑战属性 $\text{att}_i, \text{att}_j \notin A^{\text{Ext}}$ ， $\mathcal{A}$ 依然无法在多项式时间内以不可忽略的优势 ε 区分属性 att_i 对应用户的共享密钥与一个相同长度的随机值。式(4)和式(5)分别给出了安全模型和攻击者优势的形式化定义。

$$\begin{aligned}
 & \text{Exp}_{\mathcal{A}}^{\text{sk-secure}}(\lambda) \\
 & \text{param} \leftarrow \text{Setup}(\lambda); \\
 & \text{att}_i \leftarrow \mathcal{A}^{\text{Extract}(\text{att}_i), \text{Reveal}(\text{att}_i)}(\text{param}); \\
 & \beta \leftarrow_R \{0, 1\}, r_0 \leftarrow_R Z_p^*, r_1 = \mathcal{K}, R = r_\beta \\
 & \beta' \leftarrow \mathcal{A}(\text{param}, \text{att}_i, R) \\
 & \text{if } (\beta = \beta') \\
 & \quad \text{return}(1) \\
 & \text{else} \\
 & \quad \text{return}(0)
 \end{aligned} \quad (4)$$

$$\text{Adv}_{\mathcal{A}}^{\text{sk-secure}}(\lambda) = \left| \Pr[\text{Exp}_{\mathcal{A}}^{\text{sk-secure}}(\lambda) = 1] - \frac{1}{2} \right| \quad (5)$$

4 方案设计

4.1 基于前缀谓词策略的密钥分配协议

基于经典的 GGM 伪随机数生成器^[12]，本文提出了一种前缀谓词策略的密钥分配协议。协议具体包括以下 4 个步骤。

1) 初始化 $\text{Setup}(\lambda)$ ：输入系统安全参数 λ ，返回系统参数 $G_K(s)$ 以及主私钥 K 。

2) 约束伪随机函数构建：给定一个输入为 1 位的 GGM 函数 $G_K(s) = s_0 \parallel s_1$ ，该函数输入 $s = 0$ 时输出 s_0 ，输入 $s = 1$ 时输出 s_1 。由函数 $G_K(s)$ 可以扩展为一个输入长度为 n 的伪随机函数 $F: K \times \{0, 1\}^n \rightarrow Y$ 。函数 $G_K(s)$ 的扩展如图 2 所示。

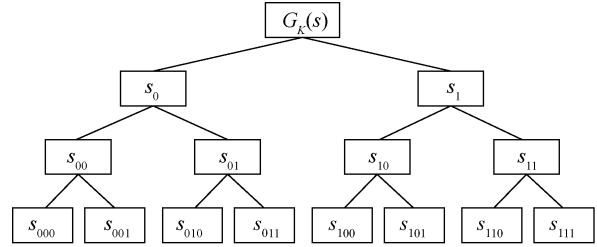


图2 基于扩展 GGM 函数的伪随机函数
Figure 2 The construction of the cPRF based on the extension of the GGM function

具体来说，扩展过程可以用一个二叉树表示，二叉树的根节点表示初始的输入值，即伪随机数生成器的初始密钥。之后，根据输入为 0 或 1，二叉树向下不断迭代扩展。每个节点的左孩子节点为输入是 0 时的计算结果，右孩子节点为输入是 1 时的计算结果。每一轮的计算结果为下一层计算的输入密钥。

式(6)定义了一个输入为 $X \in \{0, 1\}^n$ 时，基于 $G_K(s)$ 的伪随机函数 $F: K \times X \rightarrow Y$ 构建过程。

$$K \xrightarrow{G(K)[x_0]} K_1 \xrightarrow{G(K_1)[x_1]} K_2 \xrightarrow{G(K_2)[x_2]} K_3 \xrightarrow{\dots} K_n \quad (6)$$

3) 约束密钥生成算法：密钥发布者可以提前设定一个前缀属性，该属性可以形式化表示为一个前 l 位受约束的向量 $\mathbf{v} \in \{0, 1\}^{n-l}$ ，基于该向量可以得到一个前缀约束的伪随机函数。具体来说，根据用户提交的属性 att_i ，判断 att_i 与约束向量 $\mathbf{v}$ 的前 l 位是否匹配，如果不匹配，则退出。如果匹配，则基于步骤 2) 由 $G_K(s)$ 构造的伪随机函数，计算约束密钥 K_l 。约束密钥为式(6)中，第 l 轮迭代后得到的中间密钥 K_l 。

4) 共享密钥生成算法：持有约束密钥 K_l 的用户可以用该约束密钥 K_l 以及一个定期更新的公共字符串 T 计算共享密钥的值。式(7)为具体的计算过程，该值即为共享密钥 $\mathcal{K}$ 。

$$\mathcal{K} = \text{PRF}(K_l, T) = \text{PRF}(K, T) \quad (7)$$

4.2 基于位固定谓词策略的密钥分配协议

基于多线性对, 本文提出了一种位固定谓词策略的密钥分配协议, 协议具体包括以下 4 个步骤。

1) 初始化 $\text{Setup}(\lambda, n)$: 输入系统安全参数 λ , 伪随机函数输入位数 n , 返回系统参数 $\mathcal{G}(1^\lambda, n)$, 由系统参数 $\mathcal{G}(1^\lambda, n)$ 可以生成 n 个 p 阶循环群 $G = (G_1, G_2, G_3, \dots, G_n)$, 其生成元分别为 $g_1, g_2, g_3, \dots, g_n$, 并令 $g = g_1$ 。密钥发布者选取随机数 $\alpha \in \mathbb{Z}_p^*$ 。为了构建一个输入长度为 n 的位固定谓词策略的密钥分配协议, 密钥发布者需选取 n 组随机数 $(\beta_{1,0}, \beta_{1,1}), (\beta_{2,0}, \beta_{2,1}), (\beta_{3,0}, \beta_{3,1}), \dots, (\beta_{n,0}, \beta_{n,1}) \in \mathbb{Z}_p^{*2}$, 并计算 $D_{i,b} = g^{\beta_{i,b}}, i \in \{0, 1\}$ 。协议的主私钥为 $G = (G_1, G_2, G_3, \dots, G_n)$, $\alpha \in \mathbb{Z}_p^*$, $(\beta_{1,0}, \beta_{1,1}), (\beta_{2,0}, \beta_{2,1}), (\beta_{3,0}, \beta_{3,1}), \dots, (\beta_{n,0}, \beta_{n,1}) \in \mathbb{Z}_p^{*2}$, $D_{i,b} = g^{\beta_{i,b}}, i \in \{0, 1\}$ 。

2) 共享密钥计算: 对于输入 $\mathcal{X}$, 属性符合要求的用户需要计算的共享密钥如式(8)所示。

$$F(k, \mathcal{X}) = g_{n+1}^{\alpha \prod_{i=1}^n \beta_{i, x_i}} \quad (8)$$

其中, $\mathcal{X} = \{x_1, x_2, x_3, \dots, x_n\}$, x_i 表示输入的第 i 位。

3) 约束密钥生成算法: 密钥发布者可以提前设定一个位固定属性, 该属性可以形式化表示为一个 n 位向量 $\mathbf{v} \in \{0, 1, ?\}^n$ 。向量 $\mathbf{v}$ 代表一个能够计算共享密钥的属性模式, 基于该向量可以得到一个位固定的伪随机函数。具体来说, 令 I 表示向量 $\mathbf{v}$ 的非“?”位的下标所组成的集合。部分约束密钥按照式(9)计算。

$$k'_v = g_{1+|I|}^{\alpha \prod_{i \in I} \beta_{i, v_i}} \quad (9)$$

约束密钥 $k_v = (k'_v, D_{i,b}), i \notin I, b \in \{0, 1\}$ 由部分约束密钥 k'_v 和非约束位所对应的 $D_{i,b} (i \notin I, b \in \{0, 1\})$ 组成。

4) 约束伪随机函数求值算法: 持有约束密钥 k_v 的用户可以选定一个定期更新的公共字符串 S , 基于 S 计算中间值 $T = g_{n-|I|}^{\prod_{i=1, i \notin I}^n \beta_{i, x_i}}$, 其中, x_i 代表 S 的第 i 位。基于约束密钥 k_v , 共享密钥按照式(10)进行计算。

$$\mathcal{K} = e(T, k'_v) = e(g_{n-|I|}^{\prod_{i=1, i \notin I}^n \beta_{i, x_i}}, g_{1+|I|}^{\alpha \prod_{i \in I} \beta_{i, v_i}}) = g_{n+1}^{\alpha \prod_{i=1}^n \beta_{i, x_i}} \quad (10)$$

5 安全分析

基于 GGM 方案的安全性和 K-MDDH 假设, 本节证明基于前缀谓词策略的密钥分配协议以及基于位固定谓词策略的密钥分配协议的安全性。

5.1 基于前缀谓词密钥分配协议的安全性

定理 1 如果 GGM 方案是安全的, 则本文设计的基于前缀谓词策略的密钥分配协议是安全的。

证明 GGM 方案的安全性指对于函数 $G_K(s)$ 在没有获得运行密钥 K 的情况下, 攻击者 $\mathcal{C}$ 无法区分 $G_K(s)$ 的输出与一个与其相同长度的随机值。假定攻击者 $\mathcal{A}$ 能以不可忽略的优势 ε 攻破协议, 则在安全模型所定义的游戏, 存在一个挑战者 $\mathcal{C}$, $\mathcal{C}$ 通过与 $\mathcal{A}$ 交互, 利用 $\mathcal{A}$ 对协议的攻击优势以不可忽略的优势 ε_1 攻破 GGM 方案的安全性。 $\mathcal{C}$ 与 $\mathcal{A}$ 交互的过程可以用游戏 Game_0^{PP} 定义。

Game_0^{PP} : $\mathcal{C}$ 按照协议描述进行初始化操作, 并将公共参数传输给攻击者 $\mathcal{A}$ 。 $\mathcal{A}$ 在获得协议公共参数后, 根据安全模型定义, 可以向 $\mathcal{C}$ 进行下述询问。

1) 私钥提取询问 $\text{Extract}(\text{att}_l)$: $\mathcal{A}$ 选择 $l \in [1, n]$ 以及一个前 l 位受约束的向量 $\mathbf{v} \in \{0, 1\}^l ?^{n-l}$, $\mathcal{C}$ 返回向量 $\mathbf{v} \in \{0, 1\}^l ?^{n-l}$ 所对应的约束密钥 K_l 。

2) 共享密钥提取询问 $\text{Reveal}(\text{att}_l)$: $\mathcal{A}$ 选择一个前 l 位受约束的向量 $\mathbf{v} \in \{0, 1\}^l ?^{n-l}$, $\mathcal{C}$ 返回向量 $\mathbf{v} \in \{0, 1\}^l ?^{n-l}$ 及一个定期更新的公共字符串 T 的共享密钥 $\mathcal{K}$ 。

3) 挑战算法 $\text{Test}(\text{att}_l)$: 攻击者 $\mathcal{A}$ 对前缀约束向量 $\mathbf{v} \in \{0, 1\}^l ?^{n-l}$ 进行任意多次私钥提取询问和共享密钥提取询问后, 选取一个欲挑战的前缀约束向量 $\mathbf{v} \in \{0, 1\}^j ?^{n-l}$, 其中 $\forall l, 0 \leq j \leq l \leq n$ 。挑战者 $\mathcal{C}$ 返回一个随机值或者 $\mathbf{v} \in \{0, 1\}^j ?^{n-l}$ 对应的共享密钥。攻击者 $\mathcal{A}$ 输出猜测 $b \in \{0, 1\}$, $b = 0$ 表示 $\mathcal{A}$ 猜测获得的是随机值, $b = 1$ 表示 $\mathcal{A}$ 猜测获得的是一个共享密钥。

游戏结束后, $\mathcal{C}$ 将 $\mathcal{A}$ 的输出作为对 GGM 方案 $G_K(s)$ 在前 j 位固定时所对应约束密钥 K_j 和一

个相同长度的随机值的猜测。由此，若 $\mathcal{A}$ 攻击协议的优势 ε 不可忽略，则 $\mathcal{C}$ 区分 K_j 与一个随机值的优势 ε_1 亦不可忽略。这意味着， $\mathcal{C}$ 能以不可忽略的优势 ε_1 攻破 GGM 方案的安全性。由于 GGM 方案是安全的，由反证法可以推出本文提出的基于前缀谓词策略的密钥分配协议是安全的。

5.2 基于位固定谓词密钥分配协议的安全性

定理 2 如果 K-MDDH 问题是困难的，则本文设计的基于位固定谓词策略的密钥分配协议是安全的。

证明 假定攻击者 $\mathcal{A}$ 能以不可忽略的优势 ε 攻破协议，则在安全模型所定义的游戏，存在一个挑战者 $\mathcal{C}$ ， $\mathcal{C}$ 通过与 $\mathcal{A}$ 交互，利用 $\mathcal{A}$ 对协议的攻击优势以不可忽略的优势 ε_1 攻破 K-MDDH 假设。 $\mathcal{C}$ 与 $\mathcal{A}$ 交互的过程可以用游戏 $\text{Game}_0^{\text{BFP}}$ 定义。此外，在进行游戏前 $\mathcal{A}$ 需选定一个待挑战的属性 att_i 。

$\text{Game}_0^{\text{BFP}}$ ：首先， $\mathcal{C}$ 按照协议描述进行初始化操作。具体来说， $\mathcal{C}$ 已知 $g, g^{c_1}, g^{c_2}, g^{c_3}, \dots, g^{c_{\kappa+1}}$ ， $g_1 = g$ ，判断 T 是 $g_{\kappa}^{c_i} \in G_{\kappa}$ 或一个 G_{κ} 中的随机元素 R ，其中

$$T = \begin{cases} g_{\kappa}^{\prod_{i=1}^{\kappa+1} c_i}, b=1 \\ R, b=0 \end{cases}$$

之后， $\mathcal{C}$ 按照如下方式构建协议：选取 n 个随机数 $z_1, z_2, z_3, \dots, z_n \in Z_p^*$ ，根据 att_i ，如果 $\text{att}_i[i] = b$ ，则令 $D_{i,b} = g^{c_i}$ ；如果 $\text{att}_i[i] \neq b$ ，则令 $D_{i,b} = g^{z_i}$ 。此外，令系统主私钥 $\alpha = c_{\kappa} \cdot c_{\kappa+1}$ 。最后， $\mathcal{C}$ 将公共参数传输给攻击者 $\mathcal{A}$ 。 $\mathcal{A}$ 在获得协议公共参数后，根据安全模型的定义向 $\mathcal{C}$ 进行下述询问。

1) 私钥提取询问 $\text{Extract}(\text{att}_i)$ ： $\mathcal{A}$ 可以选择任意属性 $\text{att}_i \in \{0,1,?\}^n$ 进行私钥提取询问。 $\mathcal{C}$ 在收到 $\mathcal{A}$ 的私钥提取询问后令 V 为 att_i 中所有不为“？”的下标组成的集合。之后，对比 att_i 的第 j 位

($j \in V$) 与 att_i 的第 j 位 ($j \in V$)。如果 $\forall j \in V$ 都有 $\text{att}_i[j] = \text{att}_i[j]$ ，则 $\mathcal{C}$ 终止。否则， $\mathcal{C}$ 将得到一个下标 j 满足 $\text{att}_i[j] \neq \text{att}_i[j]$ 。 $\mathcal{C}$ 计算 $g_2^{\alpha} = e(g^{c_{\kappa}}, g^{c_{\kappa+1}})$ ，收集所有 $D_{i,\text{att}_i[i]}, i \in V/j$ 并计算部分约束密钥 $k'_{\text{att}_i} = g_{1+|V|}^{\alpha \cdot \prod_{i \in V/j} d_{i,\text{att}_i[i]}}$ 。最终， $\mathcal{C}$ 返回约束密钥 $(k'_{\text{att}_i}, D_{i,b}), i \notin V, b = \{0,1\}$ 。

2) 共享密钥提取询问 $\text{Reveal}(\text{att}_i)$ ：由于所设计的协议中计算共享密钥的公共参数是公开的，所以获得约束密钥的攻击者 $\mathcal{A}$ 可以计算任意共享密钥。因此，共享密钥询问等同于约束密钥询问。

3) 挑战算法 $\text{Test}(\text{att}_i)$ ：攻击者 $\mathcal{A}$ 在对任意属性 $\text{att}_i \in \{0,1,?\}^n$ 进行私钥提取询问后，向属性 att_i 发起挑战。攻击者 $\mathcal{A}$ 输出猜测 $b = \{0,1\}$ ， $b=0$ 表示 $\mathcal{A}$ 猜测自己获得的是随机值， $b=1$ 表示 $\mathcal{A}$ 猜测自己获得的是一个共享密钥。 $\mathcal{C}$ 则将 $\mathcal{A}$ 输出的 b 直接作为对 K-MDDH 问题的猜测。

若 $\mathcal{A}$ 攻击协议的优势 ε 不可忽略，则 $\mathcal{C}$ 能以相同的优势 ε_1 攻破 K-MDDH 假设。由于 K-MDDH 假设是困难的，由反证法可以推出本文提出的基于位固定谓词策略的密钥分配协议是安全的。

5.3 性能分析

在性能分析方面，本文选取了两个最新的密钥分配协议与本文所提出的协议进行分析对比。表 2 展示了具体的分析结果，由表 2 可知，相对于文献[9]协议，本文所提出的协议能够支持多用户的密钥分配。此外，本文所提出的协议可以在公开信道中安全执行。与文献[10]协议相比，本文在安全模型中正式地定义了攻击者所具备的能力并基于 ROM 模型形式化证明了所提出协议的安全性。

6 结束语

针对边缘计算的隐私保护密钥分配问题，本文提出了两种基于策略的密钥分配协议，特别地，基于约束伪随机函数和谓词，分别提出了基于前缀谓

表 2 安全属性分析
Table 2 The analysis of the security requirement

协议	信道属性	用户数量	安全性	密钥语义安全	用户隐私安全	抗身份伪装攻击
文献[9]	安全信道	2	非形式化安全	✓	×	×
文献[10]	公开信道	n	非形式化安全	✓	×	×
本文	公开信道	n	形式化安全	✓	✓	✓

词的密钥分配协议和基于位固定谓词的密钥分配协议。其中, 基于前缀谓词的密钥分配协议利用经典的 GGM 方案实现了面向边缘节点资源受限环境的高效轻量密钥分配; 基于位固定谓词的密钥分配协议利用多线性对实现了面向灵活动态环境的密钥分配。在此基础上, 本文形式化定义了协议安全模型并基于 ROM 形式化证明了所提出协议的安全性。

参考文献:

- [1] 潘爱民. 创新物联网 OS 安全应对 IoT 风险[J]. 中国信息安全, 2020(2): 44-51.
PAN A M. Resisting IOT risk by the innovation of the IOT OS security[J]. China Information Security, 2020(2): 44-51.
- [2] 施巍松, 张星洲, 王一帆, 等. 边缘计算: 现状与展望[J]. 计算机研究与发展, 2019, 56(1): 69-89.
SHI W S, ZHANG X Z, WANG Y F, et al. Edge computing: state-of-the-art and future directions[J]. Journal of Computer Research and Development, 2019, 56(1): 69-89.
- [3] 彭维平, 熊长可, 贺军义, 等. 边缘计算场景下车联网身份隐私保护方案研究[J]. 小型微型计算机系统, 2020, 41(11): 2399-2406.
PENG W P, XIONG C K, HE J Y, et al. Research on the identity privacy protection scheme of internet of vehicles in edge computing scenario[J]. Journal of Chinese Computer Systems, 2020, 41(11): 2399-2406.
- [4] QIU H, QIU M, LU Z, et al. An efficient key distribution system for data fusion in V2X heterogeneous networks[J]. Information Fusion, 2019, 50: 212-220.
- [5] RAYA M, HUBAUX J P. Securing vehicular ad hoc networks[J]. Journal of Computer Security, 2007, 15(1): 39-68.
- [6] SHEN J, ZHOU T Q, HE D B, et al. Block design-based key agreement for group data sharing in cloud computing[J]. IEEE Transactions on Dependable and Secure Computing, 2017.
- [7] SHEN J, ZHOU T Q, CHEN X F, et al. Anonymous and traceable group data sharing in cloud computing[J]. IEEE Transactions on Information Forensics and Security, 2017, 13(4): 912-925.
- [8] 周天祺, 杨惠杰, 沈剑. 车联网中支持动态操作的密钥协商协议[J]. 密码学报, 2020, 7(3): 375-388.
ZHOU T Q, YANG H J, SHEN J. Key agreement protocol with dynamic property for VANETs[J]. Journal of Cryptologic Research, 2020, 7(3): 375-388.
- [9] 单莉. 车联网中面向 V2V 安全即时通信的密钥分配方案设计[J]. 信息安全与通信保密, 2020(10): 107-113.
SHAN L. Key distribution program design for V2V instant secure messaging in Internet of Vehicles[J]. Information Security and Communications Privacy, 2020(10): 107-113.
- [10] 徐堂炜, 张海璐, 刘楚环, 等. 基于强化学习的低时延车联网群密钥分配管理技术[J]. 网络与信息安全学报, 2020, 6(5): 119-125.
XU T W, ZHANG H L, LIU C H, et al. Reinforcement learning based group key agreement scheme with reduced latency for VANET[J]. Chinese Journal of Network and Information Security, 2020, 6(5): 119-125.
- [11] WANG D, WANG P. Two birds with one stone: two-factor authentication with security beyond conventional bound[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 15(4): 708-722.
- [12] 王晨宇, 汪定, 王菲菲, 等. 面向多网关的无线传感器网络多因素认证协议[J]. 计算机学报, 2020, 43(4): 683-700.
WANG C Y, WANG D, WANG F F, et al. Multi-factor user authentication scheme for multi-gateway wireless sensor networks[J]. Chinese Journal of Computers, 2020, 43(4): 683-700.
- [13] BONEH D, WATERS B. Constrained pseudorandom functions and their applications[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2013: 280-300.
- [14] GOLDBREICH O, GOLDWASSER S, MICALI S. How to construct random functions[M]//Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali. 2019: 241-264.
- [15] GARG S, GENTRY C, HALEVI S. Candidate multilinear maps from ideal lattices[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2013: 1-17.
- [16] LI J, TANG X, WEI Z, et al. Identity-based multi-recipient public key encryption scheme and its application in IoT[J]. Mobile Networks and Applications, 2019: 1-8.
- [17] DUPONT R, ENGE A. Provably secure non-interactive key distribution based on pairings[J]. Discrete Applied Mathematics, 2006, 154(2): 270-276.
- [18] PATERSON K G, SRINIVASAN S. On the relations between non-interactive key distribution, identity-based encryption and trapdoor discrete log groups[J]. Designs, Codes and Cryptography, 2009, 52(2): 219-241.

[作者简介]



沈剑 (1985-), 男, 江苏南京人, 南京信息工程大学教授、博士生导师, 主要研究领域为数据安全、公钥密码学和云计算安全。



周天祺 (1994-), 女, 贵州黔南人, 南京信息工程大学博士生, 主要研究方向为公钥密码学和云计算安全。



王晨 (1994-), 男, 江苏无锡人, 南京信息工程大学博士生, 主要研究方向为数据安全和公钥密码学。



杨惠杰 (1995-), 女, 北京人, 南京信息工程大学博士生, 主要研究方向为公钥密码学和安全多方计算。