硕士学位论文

基于属性的凭证及其应用

ATTRIBUTE-BASED CREDENTIALS: THEORY AND APPLICATIONS

柳枫

哈尔滨工业大学

2019 年 6 月

国内图书分类号：TP393.1　　学校代码：10213
国际图书分类号：654　　密级：公开

工学硕士学位论文

基于属性的凭证及其应用

硕士研究生：柳枫
导　　师：王琦助理教授
申请学位：工学硕士
学　　科：计算机科学与技术
所在单位：南方科技大学
答辩日期：2019 年 6 月
授予学位单位：哈尔滨工业大学

Classified Index: TP393.1
U.D.C: 654

Dissertation for the Master's Degree in Engineering

ATTRIBUTE-BASED CREDENTIALS: THEORY AND APPLICATIONS

Candidate: Feng Liu
Supervisor: Prof. Qi Wang
Academic Degree Applied for: Master of Engineering
Specialty: Computer Science and Technology
Affiliation: Southern University of Science and Technology
Date of Defence: June, 2019
Degree-Conferring-Institution: Harbin Institute of Technology

摘　要

在信息产业高度发达的今天，人们在享受数字化服务带来便利的同时，服务提供商也在不断收集用户的隐私信息。如在申请某项服务时，用户通常需要提供身份信息来证明自己拥有获取此项服务的权限，服务商也就同时获取到该身份信息。要保护用户的隐私，我们可以使用一种具有匿名性质的凭证来代替传统的身份凭证。基于属性的凭证就属于这类具有匿名性质的凭证，它可以保证用户在完成验证的同时不泄露自己的隐私。像这样的凭证系统通常需要具备匿名性和可验证性，我们可以通过密码学来实现这两个基本性质。

在这篇论文中，我们首先介绍了一些重要的密码学原语，然后阐述了如何利用这些密码学原语构造基于属性的凭证系统，并简要介绍了现实中存在的系统实例。作为基于属性的凭证系统的一个重要应用，我们针对车辆自组网中的安全与隐私保护问题，并结合现有的基于属性的凭证系统的构造及特点，设计了一个高效的保护隐私的解决方案。此方案的核心是基于环签名的机制，在满足车辆自组网环境中安全需求的情况下，同时有效地保护车辆的隐私。与现有的其它基于环签名的方案不同，此方案利用了基于身份的密码学和对称密码学的优势，合理地将路边的通信设施融入到整个系统中，解决了其它基于环签名的方案中存在的列表成员的可验证性问题。通过与其它方案对比，我们总结了该提出方案的优势，并对所实现的性质进行了详细说明。

关键词：匿名凭证；基于属性的凭证；环签名；车辆自组网

Abstract

With the rapid development of information technology, while people are enjoying the convenience enabled by information technology, the service providers are collecting users' private information. For example, when a user requests service, the identity information is usually required as a proof of his/her subscription while the service providers can learn the user's identity. For the purpose of preserving privacy in certain authentication scenarios, a kind of anonymous credentials are proposed. Attribute-based credentials (ABCs) are one of these anonymous credentials, which provide a powerful tool to preserve privacy in applications, of which the two important properties: authenticity and anonymity are achieved using cryptography.

In this thesis, we first introduce some important cryptographic primitives, and show how to use these primitives to construct an ABCs system. Then we focus on the vehicular ad-hoc networks(VANETs) and propose our scheme,which is efficient and privacy-preserving. Our proposed scheme is based on ring signature scheme, and is very different from other existing schemes by combining ID-based cryptography and symmetric cryptography, and is efficient to fulfill the verification of ring members. Furthermore, we compare our proposed scheme with other existing schemes, and summarize the properties of our scheme.

Keywords: anonymous credentials, attribute-based credentials, ring signature, VANETs

目 录

第 1 章 绪论

1.1 课题的来源

在日常生活中，我们经常会不经意地泄露自己的身份信息，尤其是当我们在进行一些与身份验证相关的操作。想象这样一个场景，当我们走进酒吧去买酒时，通常需要证明自己的年龄已经大于十八岁。最直接的证明方式就是使用自己的身份证，这种做法尽管可以完成验证，但同时也存在着许多安全隐患。身份证中包含了完整的个人信息，这种直接出示的方式无疑将自己的身份信息暴露出去，从而造成个人隐私泄露的问题。

重新考虑一下这个场景，不难发现，用户只需要提供“年龄”这一个属性信息。如果用户能够在不提供完整的身份凭证的情况下，证明自己的年龄确实满足大于十八岁的条件，那么他就能最大限度地保护自己其它的身份信息不被泄露。一般情况下，当用户申请获取某项服务时，服务提供商需要用户证明其拥有获取此项服务的权限。一种保护隐私的方法是，用户只需要提供一种记录着获取这项服务所需的必要属性的凭证，服务提供商可以凭借此凭证完成对用户权限的认证。像这种能够在不暴露额外个人隐私信息的情况下完成对属性所有权的证明的凭证，我们就称之为基于属性的凭证（Attributed-Based Credentials，ABCs）。

1.2 课题的研究背景和意义

随着信息技术的不断发展，互联网已经成为了我们日常生活中不可或缺的一部分。由于网络的普及，各类互联网产品层出不穷。现有的互联网服务已经覆盖了衣食住行各个方面，我们足不出户便能享受互联网带来的便利。在这种信息产业高度发达的环境下，也存在着不少的安全隐患。尤其是以数字化形式存储的个人信息，相比于传统的纸质信息，更容易被互联网服务提供商收集、存档甚至出售给第三方组织，从而导致个人隐私信息泄露事件频频发生。比如近几年频繁发生的多起信息诈骗案件，究其根源就在于用户个人隐私信息遭到泄露。目前国内的网络黑灰产业链已达千亿规模[①]，这些网络黑灰产行业利用一些漏洞非法获取用户的信息，并通过收集用户的上网习惯，勾勒出其在现实生活中的真实状态，然后实施有针对性的诈骗。除此之外，有些商业公司也会利用用户的隐私信息来为自己牟利。2018 年，Facebook 公司就被指出通过收集用户的个人资料数据并将这些数

① http://finance.people.com.cn/n1/2018/0823/c1004-30245368.html

据出售给剑桥分析公司[①]。剑桥分析公司使用这些数据在美国总统大选期间来推送具有倾向性的广告，间接地影响美国大选。这类事件的频繁发生，更加凸显保护隐私的重要性。

在大多数场景下，互联网服务提供商没有必要收集用户的隐私信息。那么我们是什么情况下提交了自己的个人隐私数据呢？通常是向服务提供商验证自己的身份以获取某项服务的时候。因此我们需要关注的是如何在不泄露隐私的情况下，完成对拥有此项服务使用权限的证明。这已成为隐私保护领域面临的新挑战。

基于属性的凭证正是为了解决这类问题而提出的。当我们在证明自己拥有某项服务的使用权限时，可以根据服务提供商要求必须满足的基本属性，提供相应的基于属性的凭证。这类凭证与传统的身份凭证不同，它只记录了用户的一些属性信息，服务提供商通过验证这些属性来确定用户是否具备相应权限。仅仅通过基于属性的凭证，服务提供商无法将其与用户的真实身份关联起来。这种方式能够在最大程度上保护用户的隐私，从根源上防止用户个人隐私数据的泄露。从服务提供商的角度来说，使用这类的凭证系统能很好地取得用户的信任，从而吸引更多的用户使用他们提供的服务。这种以匿名的形式进行交互的方式在现实生活场景中有很广泛的应用。目前的绝大多数服务提供商都不可避免地收集用户的个人信息，而且随着大数据、物联网及数据挖掘等技术的发展，用户也正面临着越来越多的安全隐患。基于属性的匿名凭证一旦得到广泛应用，可以有效地保护用户的个人隐私。

但是要构建一个这样的系统是一件棘手的事，需要结合许多密码学的理论和工具。传统的构造方案主要关注于协议的设计，距离实际应用场景还有一定的距离。现有的基于属性的凭证系统已经能很好地实现匿名等性质，但在效率方面还有待提高。随着一些新的密码学原语的提出，基于属性的凭证系统的构造方案也有了新的进展。如何设计一个高效且与具有实际应用价值的基于属性的凭证系统，是目前热门的研究内容。

1.3 国内外研究进展及成果

基于属性的凭证是由匿名凭证（Anonymous Credentials）发展而来，第一个真正意义上可行的匿名凭证系统 IdeMix 是由 Camenisch 与 Herreweghen 于 2002 年提出来的[1]。经过十多年的发展，许多不同的方案相继被提出。但由于研究的视角不同，国内外研究工作的侧重点也不同。

国外在隐私保护方面的研究发展较早，处于领先地位。目前国外的研究工作主

① https://wallstreetcn.com/articles/3256863

要集中在设计具有实际意义的基于属性的凭证系统平台,如 ABC4Trust[2]（Attribute-Based Credentials for Trust）、IRMA[3]（I Reveal My Attributes）。与传统的 IdeMix 系统不同，这些方案不再停留在协议的设计，更多的是提供了一套完整的开发框架，开发者可以通过使用这些平台来开发自己的应用。另外，一些新颖的匿名凭证如去中心化的匿名凭证[4]，可委托的基于属性的凭证[5] 等具有特殊应用场景的方案也相继被提出。与此同时，还出现了将匿名凭证系统应用到智慧城市[6]，智能交通[7] 和物联网[8] 等特定应用场景中的构想。

相较于国外，国内对这类的研究相对较少，比较相关的有一些像环签名、聚合签名等具有匿名性质的签名方案[9,10]，但没有一般化的匿名凭证的构造方案。另外，国内也有关于直接匿名证明（Direct Anonymous Attestation）的方案的构建[9]，并有基于直接匿名证明方案在电子现金系统等商务系统方面具体应用[11,12]。

1.4 主要研究内容

关于本课题的主要研究内容，我们可以从以下三个部分分别进行阐述。

第一部分，我们将主要介绍实现匿名凭证的密码学基础。要构造一个匿名凭证系统，许多密码学原语需要被用到。这些密码学原语包括数字签名 (Digital Signature)、零知识证明 (Zero-Knowledge Proofs)、承诺机制 (Commitment Schemes) 及密码哈希函数（Cryptographic Hash Function）等。尤其是对于数字签名，还需要进一步介绍具备特殊性质的签名方案，如盲签名 (Blind Signature)、群签名 (Group Signature)、环签名 (Ring Signature) 以及基于属性的签名 (Attribute-Based Signature) 等。在这一部分，我们还将着重介绍实现这些数字签名的椭圆曲线公钥密码机制，包括双线性配对（Bilinear Pairing）及其相关的性质等内容。

对于第二部分，首先我们将调研匿名凭证的相关工作，着重关注近些年来有关基于属性的凭证的理论原型，并进一步分析这些原型的优势与劣势，以及在现实生活场景中的应用。同时我们将关注近些年比较成熟的基于属性的凭证系统，理解现有方案的构建框架。

第三部分的重点是对应用场景的研究。具体地说，我们将考虑车辆自组网的环境，并对该环境中存在的安全与隐私保护问题进行充分调研。通过分析现有的一些方案，找到尚待解决的问题，再结合之前的研究工作，尝试把基于属性的凭证系统中的优势用到车辆自组网的环境中，提出我们的解决方案。

此后，我们还要对提出的方案进行充分的理论分析。一方面要在分析其优势的基础上，对满足的性质给出具体的证明。在另一方面，通过具体的实验测试，分析其效率，并与其它相近方案做比较，最后对已完成的工作进行总结。

第 2 章 背景知识及相关密码学原语介绍

在这一章中，我们主要介绍一些基本的密码学原语，包括对称和非对称密码体制、数字签名、双线性映射、环签名、零知识证明、承诺机制及密码哈希函数。另外我们还介绍了第四章中需要使用的两个方案，一个是 2001 年 Boneh 和 Franklin 提出的基于身份的加密方案[13]，另一个是 2005 年由 Chow，Yiu 和 Hui 提出的基于身份的环签名方案[14]。

2.1 对称密码体制

对称密码体制，又称私钥密码体制，也就是说在这种密码体制中，密钥是不公开的。“对称”指的是通信双方拥有相同的密钥，密钥通常是被用于加密和解密信息。对称密码体制可以提供数据加解密和信息验证两种功能，分别用于保证数据的安全性和完整性。在本文中，我们使用 $\mathcal{ENC}(\cdot)$ 和 $\mathcal{DEC}(\cdot)$ 表示现实生活中的对称加密和解密算法，如 AES 算法。

假设明文空间为 $\mathcal{M}$，密文空间为 $\mathcal{C}$，密钥空间为 $\mathcal{K}$。在拥有对称密钥 $k \in \mathcal{K}$ 和明文 $m \in \mathcal{M}$ 的情况下，加密明文 m 的过程可以表示为：

$$c = \mathcal{ENC}_k(m) \tag{2-1}$$

类似地，解密密文 c 的过程可以表示为：

$$m' = \mathcal{DEC}_k(c) \tag{2-2}$$

在使用同一个密钥 k 的情况下，我们有 $m' = m$ 始终成立。

通信双方能够借助加密和解密算法为信息的安全性提供保障，即使它们是在不安全的信道中进行传输的。由于信道中传输的都是密文，窃听者并不能从中获取有用的信息，换句话说就是能够很好地防止被动攻击。但是仅仅依赖加密和解密不能保证传输信息的完整性，我们还需要防止传输的信息被篡改。像这种可以篡改消息的攻击方式我们一般称为主动攻击。

在对称密码体制中，为了确保能够抵抗主动攻击，通常需要使用消息验证码（Message Authentication Code，MAC）。记 $\mathcal{HMAC}(\cdot)$ 为一个基于哈希函数的消息验证码算法。那么，对于消息 m，生成消息验证码的过程可以表示为：

$$\Sigma = \mathcal{HMAC}_k(m) \tag{2-3}$$

欲使通信双方在进行信息传输的过程中能抵抗主动攻击，一般先加密明文，再对加密后的密文生成消息验证码（Encrypt-then-MAC）[15]。

2.2 公钥密码体制

公钥密码，又称非对称密码，所谓的“非对称”是相对“对称密码学”而言的，意思是在这种体制中存在公钥和私钥这两种密钥。公钥一般是公开的，所有人都可见的，被用于对信息的加密或验证；私钥则是用户自己私密保管的，一般是用来解密或签名。在对称密码体制中，加密和解密使用的是同一个密钥，这个密钥是需要通信双方保密的，因此存在着密钥协商的问题，即如何安全地为通信双方传递这个密钥。在公钥密码体制中就不存在这个问题，因为每个用户可以产生一对密钥，不用密钥协商，只需要公开自己的公钥，同时保管好自己的私钥。这样的做法显然简化了密钥的管理。

公钥密码体制主要提供公钥加密和数字签名两种功能。在效率方面，公钥加密方案不如对称加密方案。因此在实际生活中，一般使用公钥加密机制来发起通信，通过三次握手协议完成密钥协商。在通信双方获取到相同密钥时，再使用对称密码机制进行数据的传输。

在安全性方面，公钥密码体制主要依赖于数论中的困难问题假设，比如大整数分解问题和离散对数问题。在现代密码学体系中，我们称一个问题是困难问题，意味着对于所有概率多项式时间（Probabilistic Polynomial Time）的算法 $\mathcal{A}$ 来说，通过 $\mathcal{A}$ 来解决这个困难问题的概率总是可以忽略不计的。在这里，我们使用 $\mathsf{negl}(n)$ 来表示一个可忽略函数，它的定义如下：

如果对于所有的正多项式函数 $p(n)$，总存在 N 使得当整数 $n > N$ 时，有

$$\mathsf{negl}(n) < \frac{1}{p(n)} \tag{2-4}$$

始终成立，那么我们称 $\mathsf{negl}(n)$ 是一个可忽略函数。

由此我们记 $\mathsf{Sol}_{\mathcal{A}}(n) = 1$ 为利用算法 $\mathcal{A}$ 成功求解一个困难问题的事件，那么对于困难问题的定义可以描述为：对于所有的概率多项式时间算法 $\mathcal{A}$，我们都可以找到一个可忽略函数 $\mathsf{negl}(n)$ 使得公式（2-5）总成立。

$$\Pr[\mathsf{Sol}_{\mathcal{A}}(n) = 1] \leq \mathsf{negl}(n) \tag{2-5}$$

第一个被提出并得到广泛应用的对称密码学算法是 RSA 算法，其安全性基于大整数分解问题。RSA 算法既能完成对信息的加密，也能实现数字签名[16]。由于易于实现等特性，RSA 算法在今天仍被广泛使用。

基于离散对数问题的主要有 ElGamal 公钥密码体制和椭圆曲线密码体制，现在的数字签名标准 DSS 就是基于 ElGamal 密码体制。而椭圆曲线密码体制是目前除了 RSA 之外，应用最为广泛的公钥密码体制之一。相比于 RSA，椭圆曲线密码可以使用长度更短的密钥来达到相同的安全程度，比较适合在存储能力有限的应用场景中。

2.3 数字签名

数字签名作为公钥密码学中的重要组成部分，主要作用是保证信息的完整性，同时也可以用于确定信息发送者身份的真实性。一般情况下，发送者使用自己的私钥对需要发送的信息进行签名，接收者可以使用发送者的公钥完成验证。一个完整的签名机制主要包含以下三个算法 $(\mathsf{Gen}, \mathsf{Sig}, \mathsf{Vrf})$，具体的过程如下：

• 初始化阶段：密钥生成算法 Gen 通过输入一个安全参数 κ 产生一对密钥 (pk, sk)，我们将这对密钥分别称为公钥和私钥。签名者可以公开公钥，并保管好私钥；

• 签名阶段：签名者运行签名算法 Sig：通过输入私钥 sk 及需要签名的信息 m，可以生成关于此消息的一个签名 σ。我们可以写成 $\sigma \leftarrow \mathsf{Sig}_{sk}(m)$ 的形式；

• 验证阶段：验证者在收到消息 m 及对应的签名 σ 后，可以通过输入签名者的公钥 pk，并运行验证算法 Vrf，从而生成一个比特 b，即 $b := \mathsf{Vrf}_{pk}(m, \sigma)$。当 $b = 1$ 时，意味着该签名是有效的；反之，$b = 0$ 则意味着该签名是无效的。

假设消息集合为 M，在数字签名中一般需要满足正确性和安全性：

正确性：对于任意的消息 $m \in M$，始终满足：

$$\mathsf{Vrf}_{pk}(m, \mathsf{Sig}_{sk}(m)) = 1 \tag{2-6}$$

安全性：安全性的含义是攻击者不能伪造出一个消息的签名，并且能通过验证者的验证。在定义安全性之前，我们需要考虑下面这个游戏：

在这个游戏中，我们有一个挑战者 C 和一个攻击者 $\mathcal{A}$，游戏分为 3 个步骤：

1. 挑战者 C 运行 Gen 算法，得到一对密钥 (pk, sk)；

2. C 将 pk 发送给 $\mathcal{A}$，$\mathcal{A}$ 通过访问预言机 $\mathsf{Sig}_{sk}(\cdot)$，可以得到所需消息的对应签名。我们把 $\mathcal{A}$ 访问过的消息集合记为 Q；

3. $\mathcal{A}$ 输出 (m, σ)，如果满足 $\mathsf{Vrf}_{pk}(m, \sigma) = 1$ 且 $m \notin Q$，则 A 在此游戏中获胜。

对任意的概率多项式时间的 $\mathcal{A}$ 来说，如果其获胜的概率是可忽略不计的（即 $\Pr[adv] \leq \mathsf{negl}$，$adv$ 为 $\mathcal{A}$ 获胜的事件），那么这个签名机制就是安全的。我们也可以称这种签名方案满足适应性选择消息的存在性不可伪造。

2.4 双线性映射

双线性映射也称双线性对，顾名思义，它的作用是把两个群中的元素映射到另一个群中[17]。一般这两个群指的是椭圆曲线上的加法群。双线性映射分为 Weil 对和 Tate 对两种类型，在早期的研究工作中，它们主要扮演着密码分析的角色。例如 MOV 攻击就是通过把椭圆曲线上的加法群中的点映射为另一个乘法群中的元素，从而将椭圆曲线上的离散对数问题归约到有限域中乘法群上的离散对数问题。

自 2000 年以后，人们开始发现利用双线性映射的特性可以构造出很多新颖有趣的方案，如三方一轮的密钥协商[18]，基于身份的密码体制[13] 和环签名[14] 方案等等。这些方案在云计算、物联网及生物识别等方面都有许多的应用实例。

在双线性映射中存在三个 q 阶循环群 $\mathbb{G}_1$，$\mathbb{G}_2$ 和 $\mathbb{G}_T$，q 是 κ 比特长的素数，其中 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 都是加法群，$\mathbb{G}_T$ 是乘法群。我们称映射 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ 是一个双线性映射，如果它满足以下这三条性质：

1. 双线性性: 对于所有的 $P \in \mathbb{G}_1$，$Q \in \mathbb{G}_2$ 且 $a, b \in \mathbb{Z}_q^*$，有 $e(aP, bQ) = e(P, Q)^{ab}$；

2. 非退化性: 存在 $P \in \mathbb{G}_1$，$Q \in \mathbb{G}_2$，满足 $e(P, Q) \neq 1$。换句话说，如果 P，Q 分别是 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 的生成元，那么 $e(P, Q)$ 也是 $\mathbb{G}_T$ 的生成元；

3. 可计算性：对于所有的 $P \in \mathbb{G}_1$，$Q \in \mathbb{G}_2$，都存在高效的算法计算 $e(P, Q)$。

特别地，如果 $\mathbb{G}_1 = \mathbb{G}_2$，即 $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$，那么我们可以称该双线性映射 e 是对称的，否则是非对称的。

双线性映射 e 的构造可以通过有限域上的超奇异椭圆曲线上的 Weil 对或 Tate 对来完成。在双线性映射上最常见的困难问题假设有计算性双线性 Diffie-Hellman 问题（Computational Bilinear Diffie-Hellman Problem，CBDH 问题）和判定双线性 Diffie-Hellman 问题（Decisional Bilinear Diffie-Hellman Problem，DBDH 问题），其中 CBDH 问题也是三方一轮的密钥协商方案的安全基础[18]。

CBDH 问题：在给定 $P \in \mathbb{G}_1$，$aQ, bQ, cQ \in \mathbb{G}_2$ 的情况下（其中 a, b, c 均为随机选取的），计算 $e(P, Q)^{abc}$。

DBDH 问题：在给定 $P \in \mathbb{G}_1$，$aQ, bQ, cQ \in \mathbb{G}_2$ 的情况下（其中 a, b, c 均为随机选取的），给定 $h \in \mathbb{G}_2$，判断 $h = e(P, Q)^{abc}$ 是否成立。

这两个问题都属于困难问题，而且都是在离散对数问题的基础上引申得到的。因此离散对数问题的困难性要大于 CBDH 问题的困难性，而 CBDH 问题的困难性大于 DBDH 问题的困难性。

在密码学的证明中，我们通常利用反证法的思想，并采用归约的方式（Proof by Reduction）来完成形式化的证明。形式化的证明通常包括困难问题假设，攻击

模型的建立和归约论断这三个基本步骤，通过给出一个攻击者的模型，把攻击者成功攻击的行为归约为可以成功求解某一个困难问题。在这个过程中，归约论断可以看做形式化的证明中最为核心的部分。

2.5 密码哈希函数

简单地说，密码哈希函数就是一种将比较长的字符串映射为一个长度固定且更短的字符串的函数，这种更短的字符串我们通常称为摘要（Digest）。密码哈希函数需要满足的一个基本性质是强抗碰撞性（Strong Collision Resilience），也就是说对于一个哈希函数 $H:\{0,1\}^{*}\rightarrow\{0,1\}^{\ell}$，很难在概率多项式时间内找到一个二元组 (x,x')，其中 $x\neq x'$，使得 $H(x)=H(x')$ 成立。由这种强抗碰撞性可以引出两个在安全上相对较弱的性质：

1. 弱抗碰撞性（Weak Collision Resilience）：对于给定的 x，很难在概率多项式时间内找到一个 $x'(x'\neq x)$，使得 $H(x)=H(x')$ 成立；

2. 单向性（One-Way）：在已知 $y\in\{0,1\}^{\ell}$ 的情况下，很难在概率多项式时间内找到一个 x，使得 $H(x)=y$ 成立。

哈希函数在日常生活中最广泛的应用是校验文件的完整性，比如消息摘要算法（Message Digest Algorithm，MD5）就是一种哈希函数。当我们在网上下载文件时，有些网站上会附带源文件的 MD5 值。在完成下载后，我们只需要利用 MD5 算法将本地文件进行一次哈希运算，再通过与源文件 MD5 值的对比，就可以知道本地的文件是否与源文件保持一致。

另外，哈希函数在数字签名中也扮演着很重要的角色。为了提高效率，在进行数字签名的时候，通常不是直接对签名信息进行签名，而是先将签名信息作一次哈希运算，再对这个哈希值进行签名。由于哈希函数的抗碰撞性质，在安全性上可以认为与直接签名具有同等效力。

在进行安全性的证明时，最常见的做法是将密码哈希函数抽象成随机预言机（Random Oracle）模型。这种思想最早是由 Bellare 和 Rogaway 于 1993 年提出来的[19]，它的出现为现代密码学中的安全证明提供了一种较为通用的方法。对于一个哈希函数 $H:\{0,1\}^{*}\rightarrow\{0,1\}^{\ell}$，如果它满足以下这三条性质：

1. 均匀性：H 输出的结果在 $\{0,1\}^{\ell}$ 上均匀分布；

2. 确定性：对于同一个输入，H 输出的结果也相同；

3. 有效性：对于给定的输入，H 总能在多项式时间内计算出结果。

那么，我们称此哈希函数 H 为随机预言机。

随机预言机是一种非常理想的模型，它满足的性质要比抗碰撞性和单向性更

强。这种理想化的模型在现实生活中是不存在的，因此我们在使用随机预言机模型证明的安全性在现实中不一定会是安全的。因为实际使用中，我们是使用密码哈希函数代替随机预言机实现的。基于随机预言机模型的证明方法可以在一定程度上说明系统的安全性，它的提出方便了对密码系统安全性的证明。尽管这种方法存在一定的缺陷，但不可否认的是许多基于随机预言机模型下被证明安全的密码系统已经得到广泛的接受[20]。我们认为只要在密码系统中使用的哈希函数没有比较大的缺陷时，基于随机预言机模型的安全证明是有效的。

2.6 零知识证明

零知识证明本质上是一种安全两方计算协议，参与者分别为证明方 P 与验证方 V。所谓的“知识”，可以看作是某个困难问题的解，一个论断或对某项服务的权限。通过零知识证明，证明方 P 可以向验证方 V 证明自己拥有某个“知识”，同时又能确保不泄露有关这个“知识”的任何有效信息，“零知识”就是由此体现出来的。这种证明方式可以让用户将一些重要的信息隐藏起来，对保护用户的隐私具有重大的意义。

零知识证明最早是由 Goldwasser，Micali 和 Rackoff 提出的[21]，它需要具备以下三个基本性质：

1. 完备性：如果 P 与 V 都是诚实，那么只要遵循这个协议则一定能让 V 相信 P 的论断；

2. 合理性：如果 P 的论断是本身错误的，那么他始终不能通过 V 的验证；

3. 零知识性：在这个证明的过程中，V 获取不了除了“这个论断是正确的”以外的任何有价值的信息。

一般地，零知识证明可以使用类似下面这种形式进行表示[22]：

$$PK\{(\alpha) : y = g^{\alpha}\} \tag{2-7}$$

它表示的是，P 在知道 y 的离散对数 α 的情况下，可以向 V 证明其知道 α 的值，但同时也能保证在完成这个证明后，V 不知道 α 具体的值是多少。完成这样的一个证明 P 与 V 要进行 3 次交互。为了提高效率，通常可以根据 Fiat 和 Shamir 提出的思路[23] 将证明的过程简化，简化之后就只需一次交互。像这种只需要一轮交互即可完成零知识证明的也被称作非交互式（Non-Interactive）零知识证明。这种方案也通常被拿来用于实现数字签名。

近几年区块链技术的大热也带动了对零知识证明在应用方面的研究。“零知识”的特性能够很好地解决隐私保护问题。尤其在个人隐私频频遭到泄露的今天，

如何保护个人隐私越来越受到人们关注，零知识证明技术则为解决这一类问题带来了一些启发。

2.7 承诺机制

承诺机制是一个用途很广泛的密码学原语，在这个机制中也是存在两类实体，我们分别用 P 和 V 来表示。P 需要做出一个选择，但他又不希望选择的内容被 V 知道，同时 V 也需要确保 P 不能随意修改他所做的选择。比如在观看一场球赛的过程中，P 事先对会获胜的球队进行预测，但他不想让 V 知道他预测的内容。等到比赛结束后，为了防止 P 作伪，V 希望 P 没有改变之前的预测内容。

为了解决这种问题，P 可以事先准备一个带锁的箱子，并妥善保管好钥匙。在比赛开始之前，先把要预测的内容写在纸上，再放进箱子里，然后将箱子交给 V。等到比赛结束后，再把箱子打开。由于 V 没有钥匙，因此不能知道承诺的内容，P 也无法修改箱子里的内容。

类似的，在承诺机制中，我们将承诺的内容用 x 表示，并用一个随机数 r 充当钥匙的角色。完成承诺机制需要使用一个承诺算法 Com，那么承诺值 y 可以表示为 $y = \mathsf{Com}(x, r)$ 的形式。P 要对 x 进行承诺的话，只需要把 y 的值公开。等到需要证明之前承诺的内容是 x 的话，只需要再把 r 公开即可。

一个承诺机制需要满足下面两个基本性质：

1. 隐藏性（Hiding）：对于任意的 x, x'，$\mathsf{Com}(x, U_n)$ 与 $\mathsf{Com}(x', U_n)$ 是不可区分的，即对于所有的概率多项式时间算法 $\mathcal{A}$，区分成功的概率是可忽略不计的；

2. 绑定性 (Binding)：对于任意给定的 y，不论 r 取什么值，最多只能找到一个 x 使得 $y = \mathsf{Com}(x, r)$ 成立。

假设 g 与 h 都是阶数为 q 的群 G 的生成元，对于随机数 $r \in_R \mathbb{Z}_q^*$，目前主要有两种常见的承诺机制方案：

1. Pedersen 承诺方案：$\mathsf{Com}(x, r) = g^x h^r \bmod q$

2. ElGamal 承诺方案：$\mathsf{Com}(x, r) = (g^x h^r \bmod q, g^r \bmod q)$

第一个方案是完美隐藏（Perfectly Hiding），计算性绑定（Computationally Binding），后一个方案是计算性隐藏（Computationally Hiding），完美绑定的（Perfectly Binding）。

2.8 基于身份的加密方案

在传统的非对称密码体制中，我们需要使用 CA（Certificate Authority）来确定公钥的身份。举个例子，当用户 Alice 在向 Bob 传递信息的过程中，需要使用 Bob

的公钥对信息进行加密。那么 Alice 就必须要对 Bob 的公钥进行验证，以确定这个公钥的拥有者就是 Bob。如何保证这个公钥的身份呢？这就是 CA 的作用。CA 通过向 Bob 签发证书，可以把 Bob 的公钥与其身份关联起来。Shamir 在 1984 年提出了一种不需要 CA 的加密和签名体制[24]，并且将其命名为基于身份的密码系统（Identity-Based Cryptosystems）。在基于身份的加密体制中，公钥一般直接与用户的身份信息有关。如 Bob 的邮箱或其邮箱的哈希值可以直接作为公钥。Alice 事先只需要知道 Bob 的邮箱就可以获得 Bob 的公钥，而且不用 CA 来保证公钥的身份，从而简化了一系列与证书相关的操作。

在基于身份的密码体制中，需要使用一个私钥解析器（Private Key Generator, PKG）来生成用户的私钥。要构建基于身份的签名机制是相对容易的，但要设计一个功能完备的基于身份的加密方案却不是那么简单。直到 2001 年，Boneh 和 Franklin 才提出第一个可证安全且功能完整的基于身份的加密方案[13]，这个方案是基于双线性映射的，其中主要包含以下 4 个算法：

1. Setup(1^κ)：对于输入的安全参数 κ，输出 $(\mathbb{G}_1, \mathbb{G}_T, P, q, e, s, PK, H_1)$。其中 $\mathbb{G}_1$ 是椭圆曲线上的加法群，$\mathbb{G}_T$ 是有限域上的乘法群，且 $\mathbb{G}_1$ 和 $\mathbb{G}_T$ 都是阶数为 q 的循环群。P 是 $\mathbb{G}_1$ 的一个生成元，$e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$ 是一个双线性映射。s 是由系统随机选取的，即 $s \in_R \mathbb{Z}_q^*$。PK 是系统的公钥，且 $PK = s \cdot P$。H_1 是一个 Map-to-Point 的密码哈希函数，且 $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$。初始化完成之后，系统将 s 作为主私钥（Master Secret Key）保存起来，并公开 $(\mathbb{G}_1, \mathbb{G}_T, P, q, e, PK, H_1)$；

2. KeyGen(ID_i)：对于身份信息为 ID_i 的用户，系统通过运行 KeyGen 算法可以为其生成一对密钥 (PID_i, PSK_i)。其中，PID_i 是作为用户的公钥，且 $PID_i = H_1(ID_i)$，PSK_i 是作为用户的私钥，且 $PSK_i = s \cdot PID_i$；

3. Enc(M, PID_i)：对于需要加密的明文信息 $M \in \mathbb{Z}_q^*$，首先随机选择 $r \in_R \mathbb{Z}_q^*$，然后输出密文 $C = (rP, M \oplus g_d^r)$，其中 $g_d = e(PID_i, PK)$；

4. Dec(C, PSK_i)：对于密文 $C = (rP, V)$，计算 $M' = V \oplus e(PSK_i, rP)$。

根据双线性映射的性质，我们知道：

$$e(PSK_i, rP) = e(s \cdot PID_i, P) = e(r \cdot PID_i, s \cdot P) = e(PID_i, PK)^r = g_d^r \tag{2-8}$$

因此很容易可以得出 $M' = M$。另外，此方案已经被证明在 CBDH 困难问题假设下，满足 CCA 安全（即能够抵御主动攻击）。

2.9 环签名

环签名是一种具有匿名性质的签名体制，它最早是由 Rivest, Shamir 和 Tauman

于 2001 年提出的[25]。在传统的签名体制中，验证方需要使用签名者的公钥来验证信息。从某种程度上来看，这就暴露了用户的身份信息（因为用户的公钥与身份存在着一定的关联性）。而在环签名体制中，签名者先需要收集一定数量的公钥，然后再用自己的私钥进行签名，并把最终得到的签名连同签名的内容及用到的公钥列表一起发送给验证者。由于验证者看到的是一组公钥，因此不能通过这一组公钥判断签名者真正的身份。

环签名的提出很大程度上受到了群签名的启发[26]，二者都保证了验证者只知道“此签名为群体中某个成员生成”这一事实，从而很好地保护了用户的隐私。它们之间最大的不同在于，在群签名体制中存在着群管理员，而群管理员拥有着最高的权限，能够移除旧群成员及为新群成员分配密钥。在环签名中不存在这样的管理员，也不需要环成员的合作，只需要自己来组建一个群体，因此具有很强的自发性。

这里我们主要介绍一下由 Chow，Yiu 和 Hui 等人于 2005 年提出的基于身份的环签名方案[14]。这个方案也是在双线性映射上构造的，主要包括以下 4 个算法：

1. Setup(1^κ)：对于输入的安全参数 κ，输出 $(\mathbb{G}_1, \mathbb{G}_T, P, q, e, s, PK, H_1, H_2)$，其中参数 $(\mathbb{G}_1, \mathbb{G}_T, P, q, e, s, PK, H_1)$ 与上一节基于身份的加密方案中描述的一致，H_2 是一个密码哈希函数，且 $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$。在初始化完成之后，系统将 s 作为主私钥保存起来，并公开 $(\mathbb{G}_1, \mathbb{G}_T, P, q, e, PK, H_1, H_2)$。

2. KeyGen(ID_ℓ)：与上一节类似，通过输入签名者的身份信息 ID_ℓ，系统可以生成一对密钥 (PID_ℓ, PSK_ℓ)，其中 $PID_\ell = H_1(ID_\ell)$，是作为签名者的公钥，$PSK_\ell = s \cdot PID_\ell$，是作为签名者的私钥；

3. Sign(m, PSK_ℓ, L)：对于拥有私钥 PSK_ℓ 的用户可以使用成员列表 $L = \{PID_1, PID_2, ..., PID_n\}$ 来对消息 m 进行签名，其中 $1 \leq \ell \leq n$。对于 $1 \leq i \leq n$，且 $i \neq \ell$，随机选择 $U_i \in_R \mathbb{G}_1$，然后计算 $h_i = H_2(m||L||U_i)$；再随机选取 $r'_\ell \in_R \mathbb{Z}_q^*$，并计算 $U_\ell = r'_\ell PID_\ell - \sum_{i \neq \ell}\{U_i + h_i PID_i\}$，$h_\ell = H_2(m||L||U_\ell)$ 和 $V = (h_\ell + r'_\ell)PSK_\ell$。最后输出 (m, σ, L)，其中 $\sigma = (\cup_{i=1}^n \{U_i\}, V)$；

4. Verify(m, σ, L)：对于 $1 \leq i \leq n$，计算 $h_\ell = H_2(m||L||U_i)$，然后检验 $e(PK, \sum_{i=1}^n (U_i + h_i PID_i)) = e(P, V)$ 是否成立。

这个签名方案已经被证明在随机预言机模型下具有适应性选择消息和身份下的存在性不可伪造[14]。

2.10 本章小结

在这一章中，我们首先介绍了对称与非对称密码体制以及一些基础的密码学

原语。对称与非对称密码体制都可以保障在不安全的信道中传输内容的安全性和完整性。在对称密码体制中, 通信双方需要具备相同的密钥, 并且可以使用 Encrypt-then-MAC 的方式抵抗主动攻击。非对称密码体制由于使用的是不同的密钥，相比于对称密码体制不需要事先的密钥协商，但在效率方面不如对称密码体制。因此现实生活中通常使用非对称密码体制来完成密钥的协商，通信双方可以通过这种方式得到相同的密钥。再使用对称密码的方法完成数据的传输。

非对称密码体制使用数字签名来保证数据的完整性。而基于双线性映射构造的签名方案, 得到的签名长度相对较短, 且形式较为简洁。利用双线性映射的性质我们能够相对容易地构造出具有特殊性质的加密和签名方案。基于双线性映射的方案的安全性都是基于离散对数问题，我们重点介绍了两个在双线性映射上常见的困难问题，一个是 CBDH 问题，另一个是 DBDH 问题。在后面的证明中，我们将基于这些困难问题假设完成安全性的证明。

密码哈希函数在现实生活中比较常见，它需要满足的基本性质就是强抗碰撞性。这种性质可以引申出两个相对较弱的性质：弱抗碰撞性和单向性。在进行安全性证明的时候，我们一般将其抽象为随机预言机模型。随机预言机作为一种比较“强”的理想模型，为密码学理论世界与现实世界之间搭建了一座“桥梁”。在随机预言机模型下证明的安全在一定程度上可以说明系统在现实生活中的安全性。在本文中，我们的安全性证明也是基于随机预言机模型下完成的。

零知识证明和承诺机制都是为了保护用户隐私而出现的，但二者针对的问题有很大不同。这两个密码学原语是构建一个匿名凭证系统的基础，在第三章里会讲述如何使用这两个密码学原语来实现我们所需要的特性。最后介绍的基于身份的加密和基于身份的环签名都是在第四章中需要用到的，在第四章，我们会详细描述如何把这些方案进行结合，并应用到具体的生活场景中。

这一章介绍的密码学工具在隐私保护和数据安全方面，尤其是在进行身份认证，确保数据的完整性以及实现匿名性的时候有着很广泛的应用。要构建一个基于属性的凭证系统, 我们就需要利用这些工具的优势, 以实现所需要满足的性质。

第 3 章 基于属性的凭证

基于属性的凭证是一种特殊的凭证系统。在一个凭证系统中，通常有凭证发行机构、用户及验证者这三类角色。用户可以从凭证发行机构处获取有效的凭证，验证者就可以通过校验用户凭证的真实性从而完成对用户的证明。最常见的凭证就是用户的身份证。在日常生活中，我们可以从派出所申请到有效的个人身份证。当需要进行一些与验证身份有关的操作时，如在火车站买票，我们就可以通过出示身份证的方式来验证与身份有关的信息。

那么什么是基于属性的凭证呢？首先需要解释一下属性的概念。一个人的身高、年龄、身体状况、学历等信息都可以看做这个人的属性信息。因此，我们可以将身份看做是一组属性的集合。图 3-1 表示的是 Alice 在不同场景下表现出的各个属性，而且这些属性都是直接与 Alice 的身份相关联的。

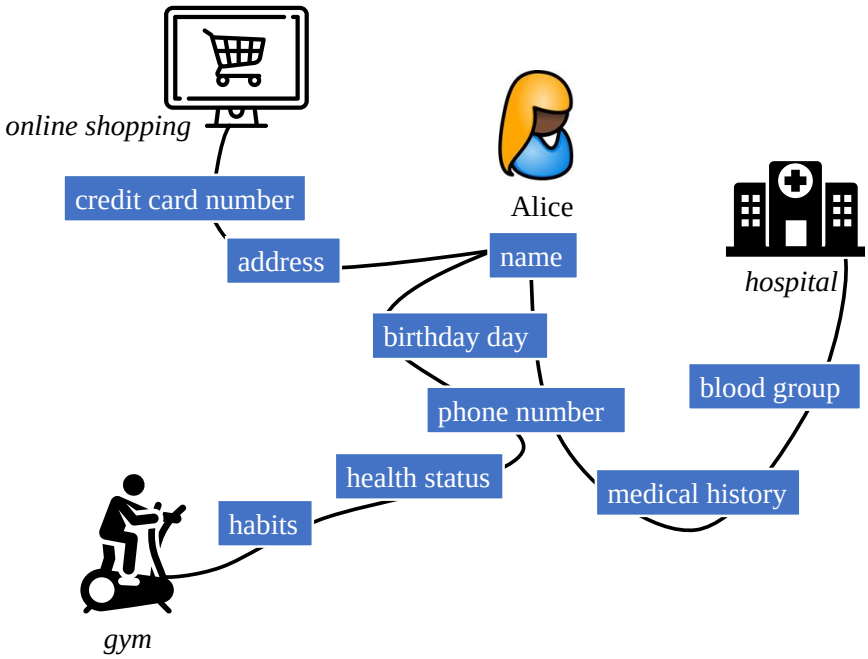

图 3-1 Alice 在不同场景下出示的属性信息

传统的凭证由于直接将属性信息与真实身份相关联，这样做会给 Alice 带来许多安全隐患。比如 Alice 在去医院看病的过程中，医院就会得知 Alice 的血型、年龄及过往病史等一系列的信息。这些信息都是直接跟 Alice 的身份挂钩，且大部分都是属于隐私的内容。假如医院的数据库遭到攻击或医院直接出售这些信息，用户的个人信息安全将会面临巨大的威胁。

基于属性的凭证的作用是切断用户的属性与用户真实身份的关联，这种性质也被称为不可关联性（Unlinkability）。因此在获取凭证的时候，用户需要的是获取对某个属性的凭证；在验证的过程中，用户只需提供必要属性的凭证即可，并且在整个验证的过程中，用户始终保持着匿名的状态。

3.1 发展历程

基于属性的凭证的概念是从匿名凭证发展而来，而匿名凭证的思想最早是由Chaum[27]于1985年提出的，他主要围绕着如何在匿名的情况下完成交易提出了自己的一系列设想。在这之后，Chaum与Evertse于1986年提出了一个解决方案[28]，这个方案需要有一个半诚实的（Semi-Honest）第三方机构[9,29]，所谓的半诚实机构意味着它可以按照规则执行协议，也不会篡改执行的数据，但可以分析这些数据。这个方案由于可行性比较差，离实际应用还有一定距离。经历了十多年的探索，同时也随着对数字签名，零知识证明等研究的不断深入，Camenisch和Lysyanskaya于2001年正式提出了第一个可行的匿名凭证方案[29]，这也是匿名凭证的概念第一次出现并被正式定义。这个方案实现了包括假名生成，凭证的生成及凭证的展示等完整的协议，同时他们也对该方案的不可伪造性，匿名性，不可关联性及可行性等基本特性给出了完整的证明。另外，他们在此基础上设计了一个扩展方案，这个扩展版的方案还满足了凭证不可出借及可撤销等与实际应用场景相关的特性。作为第一个可行方案，此方案的安全性是基于强RSA假设和离散对数假设。

这个方案在构造上很大程度上受到假名系统（Pseudonym System）[30,31]的影响，也就是说，用户在请求凭证之前，需要从凭证发行者处获取假名，然后再使用假名的方式进行交互。自第一个可行方案出现以后，关于匿名凭证的研究开始迈入新的篇章。紧接着在2002年，Camenisch与Herreweghen给出了这一方案的具体实现，也就是Idemix系统[1]。同一时期，Brands基于盲签名的方法提出了一些有关匿名验证的思想[32]，并在创建了Credentica公司之后基于此思想构建了一个匿名凭证系统U-Prove。该系统随着2008年Credentica公司被微软收购由微软继续进行研发[33]，已经成为最具代表性的匿名凭证系统之一。

匿名凭证系统的核心部分很大程度上依赖于数字签名，2001年的匿名凭证方案主要使用传统的RSA签名方案。由于双线性映射的出现推动了数字签名的发展，伴随着许多基于双线性映射的签名方案的出现[34–36]，一些新的匿名凭证的方案构造也涌现出来。基于双线性对的数字签名构造一般比较简洁，而且在同等安全条件下，签名长度相对RSA来说要短得多，如果用于匿名凭证的构造中会大大提高整个系统的效率。

2004 年 Camenisch 和 Lysyanskaya 设计了一个基于双线性对的签名方案，并基于此签名方案提出了一个匿名凭证方案[35]。在这个签名方案中，签名者可以在不知道签名内容 m 的情况下完成对 m 的签名。更准确的说，签名者只知道 m 的承诺值 $m' = \mathsf{Com}(m,r)$ 的情况下，生成对 m 的合法签名 σ。由于承诺机制满足隐藏和绑定这两个性质，在没有公开 r 的情况下，签名者无法获知所需签名的内容。因此，这种签名方案能够用在匿名凭证系统的发行凭证这一过程中。Camenisch 和 Lysyanskaya 粗略地描述了利用此签名方案来构造匿名凭证系统的思路，构造出来的匿名凭证方案也没有提供可追踪性。另一个基于此签名方案的是 Blanton 于 2008 年构造的一个匿名访问系统[37]。这个系统可以看做匿名凭证系统的特殊情况，即把凭证发行机构与验证者合并起来看做一个服务提供商。用户可以匿名地从服务商订阅服务，并以匿名的方式通过验证。同年，Akagi，Manabe 和 Okamoto 基于 Okamoto 提出的签名方案[36] 构造了一个包含完整的撤销机制的匿名凭证系统[38]。

由于普通的数字签名机制只能保证信息的完整性，并不能确保用户身份的匿名性。因此在以上提到的匿名凭证系统中，为了保证匿名性，还使用了大量的零知识证明。但是零知识证明需要多次的交互，且随着需要证明的内容增加，证明就变得越繁杂，这样就限制了匿名凭证系统的效率。尽管我们可以使用 Fiat-Shamir 协议[23] 把一个交互式的零知识证明转换成一个非交互式的零知识证明，但是这种简单的转换无法用在双线性映射上[9]，而且在安全性上需要基于随机预言机（Random Oracle）模型。

2008 年，针对双线性映射上的非交互式零知识证明协议[39] 由 Groth 和 Sahai 提出，这种零知识证明协议（GS-Proof）具有一般性，因此能够很容易地应用到其他方案构造中。自此之后，基于 GS-Proof 的匿名凭证系统方案也相继被提出[40,41]。非交互式的证明方式为匿名凭证方案的构造带来了便利，更丰富了匿名凭证的应用场景。

在匿名凭证中比较重要的部分是对属性的签名，基于属性的凭证更能体现对属性的签名这一点。自 2012 年之后，基于属性的凭证的概念开始替代了之前匿名凭证的称谓[2]，比如 ABC4Trust 这个项目中的 ABC 就是基于属性的凭证的英文缩写。现在对基于属性的凭证的研究变得越来越细致，大多是针对特定的场景下设计可行的协议或针对某一个具体的性质进行改进。比如有利用累加器（Accumulator）的方法来实现凭证撤销问题[42]，或构建一个去中心化的基于属性的凭证系统[4]，或利用结构保护的签名（Structure-Preserving Signature）来构造长度固定的凭证[43]，等等。

3.2 基本结构及性质

在前面的介绍中，我们知道数字签名和零知识证明在基于属性的凭证方案的构造上起到了很关键的作用。一般来说，凭证系统中的主要参与者可以分为用户（Users），凭证发行机构（Issuer）及验证者（Verifiers）这三类。用户拥有者许多的属性，他们可以通过向凭证发行机构发起请求，以获取相关的属性凭证。在获得相应的凭证之后，就可以通过匿名的方式提供相应的凭证给验证者，当通过验证后，用户就可以拥有获取相关服务的权限。因此验证者有时也被称做服务提供者（Service Providers），三者之间的交互过程如图 3-2 所示。

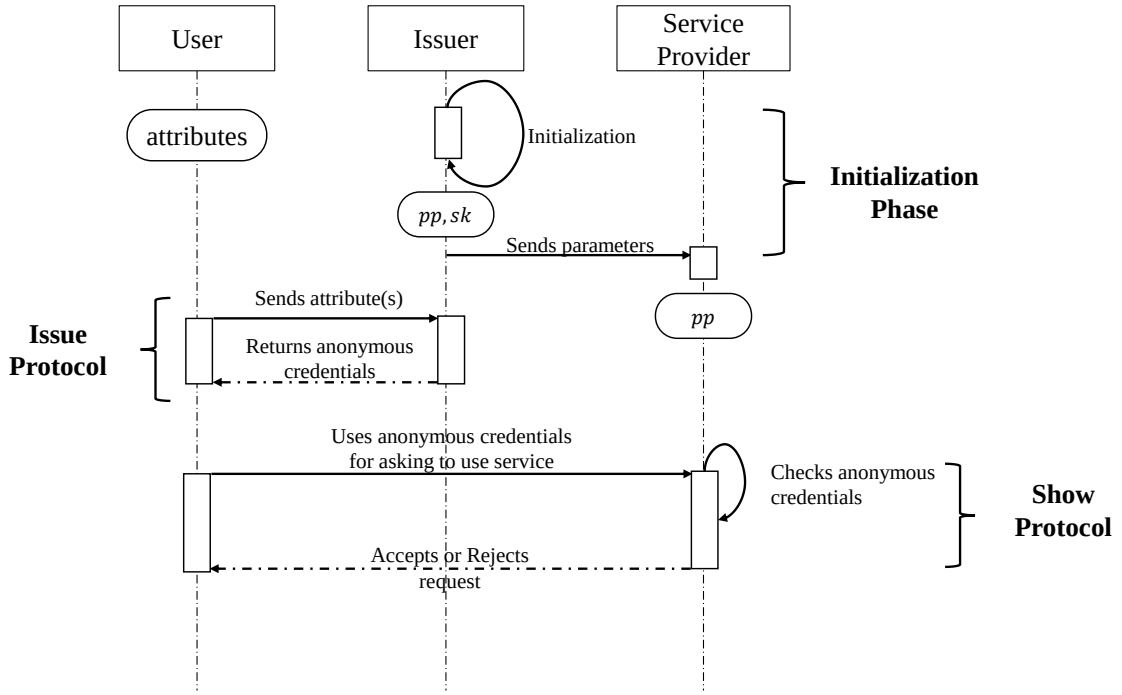

图 3-2 基于属性的凭证系统中各角色交互的序列图

为了方便说明，下面我们分别用 $\mathcal{U}$、$\mathcal{I}$ 和 $\mathcal{V}$ 来表示用户，发行机构和验证者。从图中我们可以看出，在一个基于属性的凭证系统中，主要包含初始化，发行凭证和使用凭证这三个阶段。而要构造这样一个系统，关键在于如何实现发行凭证和出示凭证这两个协议。初始化的过程一般是由 $\mathcal{I}$ 来完成，一般在输入安全参数 κ 之后，得到系统输出的公共参数 pp 及私钥 sk。$\mathcal{I}$ 需要把 sk 保管起来，并将 pp 直接公开。pp 一般包含系统的公钥及一些必要的参数，如在基于双线性映射的方案中，pp 就包含 G_1，G_T 等信息。$\mathcal{U}$ 在请求凭证之前，需要将自己的属性信息发送给 $\mathcal{I}$。当这些属性通过验证之后，$\mathcal{I}$ 可以使用 sk 对属性进行签名，并返回相应的基于属性的凭证。在一些特殊情况下，U 不是直接把属性信息传递给 $\mathcal{I}$，而是利用承诺机制对属性或一部分属性信息进行承诺，并将承诺结果发送给 $\mathcal{I}$。$\mathcal{U}$ 就可以

利用这个凭证完成对属性的证明，$\mathcal{V}$ 利用之前收到的 pp，就可以对凭证的真实性进行验证。为了确保 $\mathcal{U}$ 的身份不被泄漏，这里一般使用零知识证明的方式完成整个验证过程。

由此可知，在一个基于属性的凭证系统中，需要满足两个基本的性质，即可验证性（Authenticity）和匿名性（Anonymity）。

• 可验证性：用户只有在拥有合法的凭证的情况下才能通过 $\mathcal{V}$ 的验证。合法的凭证指的是此凭证是由 $\mathcal{U}$ 从 $\mathcal{I}$ 处获取且凭证没有被撤销。从另一个角度来说，满足可验证性即表示也满足不可伪造性，即用户 $\mathcal{U}$ 不能伪造出一个合法的凭证。可验证性是由 $\mathcal{I}$ 所使用的签名算法保证的。

• 匿名性：也可以称为身份与属性的不可关联性，即在 $\mathcal{V}$ 通过 $\mathcal{U}$ 的验证后，$\mathcal{V}$ 除了知道 $\mathcal{U}$ 拥有相应的属性信息之外，并不能知道用户的真实身份。这主要是利用零知识证明的方式来实现的，通过这种方式可以充分地保护用户隐私。

除了这两个基本的性质外，针对现实生活中的场景，我们往往还需要考虑下面这几个性质：

• 凭证的不可关联性：$\mathcal{U}$ 使用不同的凭证与 $\mathcal{V}$ 交互，对于 $\mathcal{V}$ 来说，不能判断出这多个凭证来自同一个用户。

• 可追踪性：可追踪性指的是在必要的情况下，凭证的使用者是可以被还原出来的。因此如果满足了可追踪性，那也意味着此凭证不是绝对匿名的。执行追踪的一般是凭证发行机构 $\mathcal{I}$ 或一个可信的第三方组织 $\mathcal{O}$。此外，$\mathcal{O}$ 还需要满足不能伪造凭证这一性质。

• 可撤销性：撤销一般是在凭证到期了或凭证被恶意使用的情况下执行的。要实现可撤销性，一般需要先实现可追踪性。在实际的应用场景中，可撤销还是一个很必要的特性。

3.3 相关实例

在这一节我们主要介绍已有的匿名凭证实例，这些实例包括 IdeMix、U-Prove 和 ABC4Trust。

3.3.1 IdeMix

IdeMix[1] 是第一个完整地实现了凭证的签发协议，使用协议并且支持撤销的匿名凭证系统，它是由 Camenisch 和 Herreweghen 在 2002 年设计出来的。理论上主要基于 Camenisch 与 Lysyanskaya 在 2001 年提出的第一个匿名凭证方案[29]，这个方案使用的是 RSA 密码体制，安全性依赖于大整数分解的困难性。

在这个系统中，主要的参与者还是用户 $\mathcal{U}$，凭证发行机构 $\mathcal{I}$ 和验证者 $\mathcal{V}$。其中

包含两个基本协议，即生成协议（Generation Protocol）与出示协议（Show Protocol），这两个基本协议中又包含了许多子协议。

1. **生成协议**：主要包含假名生成协议与凭证生成协议。$\mathcal{U}$ 通过向 $\mathcal{I}$ 发送请求，以获取假名。然后用户就可以使用假名从 $\mathcal{I}$ 处获取相应的凭证。

2. **出示协议**：此协议主要是 U 向 V 证明自己拥有某个凭证，从而获取使用 V 所提供的服务的权限。

在匿名凭证系统中，拥有一个可信的 $\mathcal{I}$ 是很重要的，因为 $\mathcal{I}$ 会保存着用户假名与凭证的对应关系。因此，用户在与 $\mathcal{I}$ 请求凭证的时候，可以每次选择不同的假名，这样能避免凭证与真实身份之间的关联。$\mathcal{V}$ 作为服务提供者，可以看作一个提供在线视频的网站，或一个在线购物商城。利用此系统，用户就可以用匿名的形式获取相关在线服务。IdeMix 系统不仅可以支持线上的服务，也可以支持离线的服务，如在智能卡上的应用[44]。

3.3.2 U-Prove

U-Prove 是微软公司开发的匿名凭证系统，它主要基于公钥密码学，椭圆曲线和哈希函数。系统中也存在用户 $\mathcal{U}$，凭证发行者 $\mathcal{I}$ 以及验证者 $\mathcal{V}$ 这三类角色。与 IdeMix 类似，U-Prove 中也包含生成和出示这两个基本的协议，但细节有所不同。

1. **生成协议**：$\mathcal{U}$ 从 $\mathcal{V}$ 出获取一个 token。

2. **出示协议**：$\mathcal{U}$ 使用 token 通过 $\mathcal{V}$ 的验证。

这里的 token 就包含了用户的属性信息。通过使用一些密码学的方法，可以保证 token 不被篡改。在 U-Porve 中，发行者 $\mathcal{I}$ 使用的是盲签名的方式，用户 $\mathcal{U}$ 则采取零知识证明的方式与 $\mathcal{V}$ 进行交互。此系统很好地保证了 token 与用户身份的不可关联性，但是如果多次使用同一个 token 则会破坏此不可关联性。因此用户在每次验证前都需要使用一个新的 token，只有这样才能确保完全的不可关联。

3.3.3 ABC4Trust

ABC4Trust，全称为 Attribute-Based Credential for Trust，它是由欧盟资助的用来保护个人隐私的项目[2]。与前两个项目不同，ABC4Trust 不仅关注在协议的设计，更多的是为基于属性的系统构建了一个完整的开发框架。此项目为构建基于属性的凭证系统提供了一个完整的框架，它把用户 $\mathcal{U}$ 与验证者 $\mathcal{V}$ 之间交互的过程分成了三层，从上到下分别是应用层，ABC-Engine 层和 Crypto-Engine 层。

正因为这种划分，我们可以在底层使用不同的密码学协议，层与层之间只需要提供相应的 API 接口即可。ABC4Trust 为基于属性的凭证系统的构造提供了一个比较规范的框架，这大大方便了开发者的对此类凭证系统的开发。

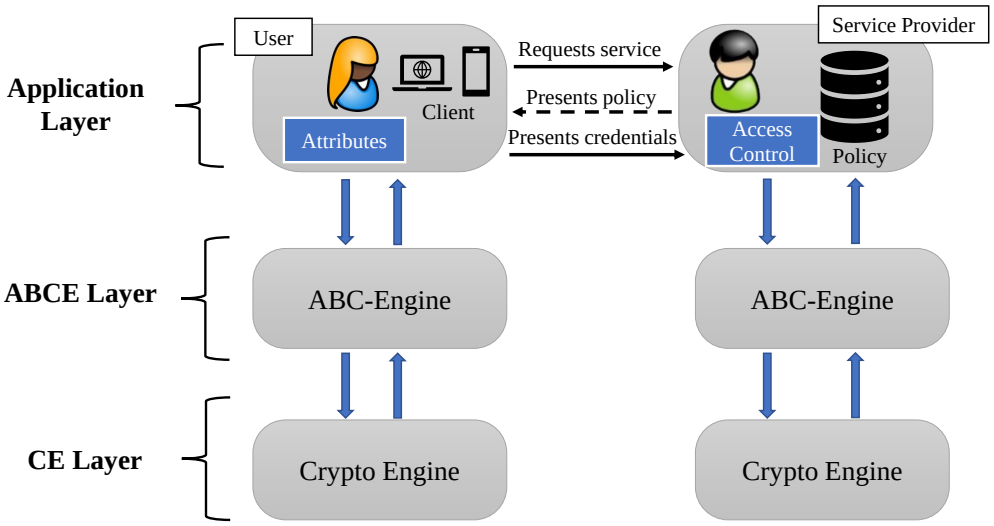

图 3-3 ABC4Trust 的基本结构

3.4 本章小结

在这一章，我们首先介绍了基于属性的凭证的发展历程，重点描述匿名凭证系统发展的几个阶段以及不同阶段的研究内容。然后我们介绍了基于属性的凭证系统的基本结构及其需要满足的一些性质。最后通过描述 IdeMix, U-Prove 和 ABC4Trust 这三个比较有代表性的现实生活中的实例，来说明匿名凭证系统的发展趋势。其中 IdeMix 深受假名系统的影响，U-Prove 利用了数字签名、承诺机制与零知识证明等方案，也是现在构建一个匿名凭证系统的常见做法。ABC4Trust 则着重于框架的设计，意在实现一套基于属性的凭证的标准。通过对这几个实例的探讨，我们可以发现，随着对匿名凭证系统研究的深入，在构造方面逐步趋于规范化。近年来，基于属性的凭证系统逐渐走向人们的生活中，在医疗、电子货币、电子身份证及物联网等方面都开始有了实际的应用。

第 4 章 基于属性的凭证在车辆自组网中的应用

在前面的章节中，我们主要介绍了基于属性的凭证的相关概念，以及在保护个人隐私方面所发挥的作用。现实生活中有很多需要身份验证的场景，大多数的场景都缺少一种保护用户隐私的措施，这会给用户本身带来很大的安全隐患。如何在确保通过验证的同时又不泄露个人的隐私信息，这已成为隐私保护领域关注的热点问题之一。车辆自组网环境就属于这类场景。

4.1 车辆自组网

车辆自组网作为智能交通系统的重要组成单元，主要是为了解决道路安全问题以及为驾乘人员提供便利而出现的。与现在热门的无人驾驶有很大不同，车辆自组网更侧重于提供辅助驾驶，主要集中在对车辆间通信的研究。这个概念很大程度上来源于物联网，因此车辆自组网可以看做是实现车联网的一个必要组件。

车与车之间通过频繁的信息交换，可以用来实现智能化的交通系统。想象在车辆自组网的环境中，我们可以通过接收其他车辆发送过来的信息，判断前面道路的拥挤状况，然后就可以挑选出最优的驾驶路线。在一些比较复杂的路况下，我们还可以通过获取附近车辆的速度与它们的位置等信息，在判断可能出现危险的情况下，及时发出警告或者车辆主动采取紧急制动措施，这样就可以避免许多交通事故的发生。因此车辆自组网与无人驾驶是相辅相成的关系，如果能很好地实现车辆自组网，那么也将会推动无人驾驶的发展。

在车辆自组网的环境中，每辆车都要求配备一个称为车载通信单元（On-Board Unit，OBU）的设备。这些设备可以将车辆的速度，位置及当前的路况等信息进行广播。道路两旁会设置一些路边单元（Road-Side Units，RSUs），这些路边单元与交通管理中心（Transportation Regulation Center，TRC）相互联通，它们也可以与车辆进行通信，以提供交通服务等信息。

因此，我们可以把车辆自组网中的通信方式粗略分为两类，一类是车辆与车辆之间的通信，即 V2V（Vehicle to Vehicle）；另一类是车辆与 RSUs 这样的基础设施进行通信，即 V2I（Vehicle to Infrastructure）。整个车辆自组网中的环境如图 4-1 所示。

由于车辆自组网是处于一种公开的环境中，因此很容易受到恶意的攻击。如果恶意的车辆广播一些虚假的交通事故或交通堵塞信息，将会给其他车辆造成误导，从而破坏交通系统的秩序。为了保障整个交通系统的安全，最简单的方法就是

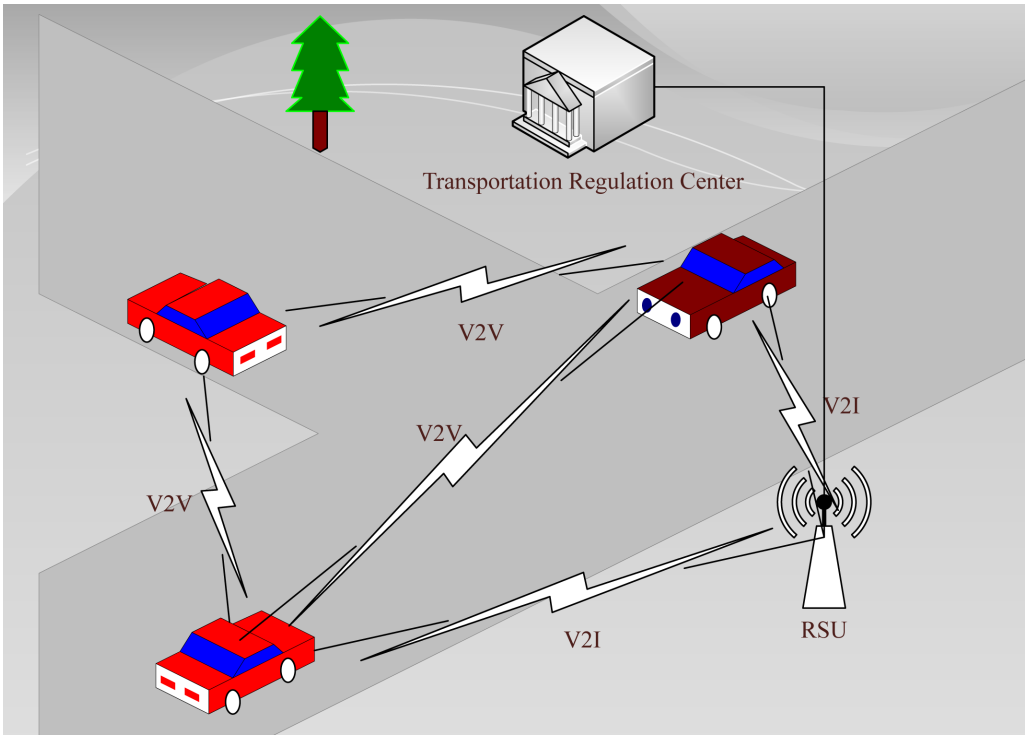

图 4-1 车辆自组网的环境

强制在广播的信息中附加可验证的车辆信息。这种做法提高了传播恶意信息的代价，虽然能够在一定程度上能确保系统的安全，但同时也侵犯了车辆的隐私。

隐私和安全是车辆自组网中重点关注的内容，隐私注重的是车辆的身份等信息不能完全暴露，而安全是指车辆广播的信息是要能被认证的。欲保护用户的隐私，那么车辆在与其它车辆或 RSUs 进行通信的时候，需要保持一种匿名的状态。但这种通信不能是绝对匿名的，在某些情况下又需要有还原出车辆真实身份的方法。如在出现了交通事故等状况时，要追踪出信息的发送者是很有必要的。从这些角度来看，我们会发现车辆自组网的环境与基于属性的凭证系统有许多相似的地方。

表 4-1 基于属性的凭证系统与车辆自组网环境的比较

	基于属性的凭证系统	车辆自组网环境
需要认证的内容	用户的属性信息	车辆的速度，路况等信息
需满足的基本性质	可验证性，匿名性	可验证性，匿名性，可追踪性，实时性
可以信任的实体	凭证发行机构	交通管理中心

如何让车辆自组网系统既能确保信息安全，又要保障个人的隐私，同时还需在某些场景中能还原用户的真实身份，这就是我们需要解决的问题。

4.2 相关工作

在车辆自组网研究的早期阶段，大多数的研究工作是围绕着如何确保信息的

可验证性。因此很自然地就有了使用数字签名的方法来防止信息的伪造[45]。但这种方案显然会暴露隐私，因为用来验证信息的公钥可以对应看做车辆的身份信息[46]。近些年的研究工作开始集中在隐私保护方面，这些工作大多是基于假名的方式。

更具体地说，根据假名表示的方法不同，这些方案可以大致分为四类[46]：第一类是基于传统的公钥密码学，第二类是使用基于身份的密码学。严格来说这两种方案都是公钥密码体制，核心思想都是用户自己申请多个公钥，然后通过频繁更换公钥的方式来维持匿名的状态。在这里，假名可以看做是由公钥来表示的。每个公钥会限制使用日期或使用次数，从而切断了公钥与真实身份之间的关联性。这两类方法最大的不同之处在于签发公钥的过程，使用基于身份的密码学可以简化密钥的签发。

然而，这种依赖频繁地更换假名的方法并不能完全地阻止对身份的追踪[47]。因此许多工作开始关注如何更换假名，这些策略包括 Mix-Context-Based 和 Mix-Zone-Based[48–50]。但是这些策略都存在一定的局限性，并不能在根本上解决问题。

第三类方案是基于群签名的，这种方案的好处是不用考虑假名更换的问题。群签名中存在着一个群管理员，群管理员可以添加或移除群成员，然后群成员可以对信息生成一个群签名。由于验证签名的时候使用的是群公钥，因此能很好地满足匿名的特性，符合车辆自组网中对可验证性及匿名性的要求。但群签名最大的弊端就是群管理员的权力过大，它可以根据签名信息直接获取签名者的身份。因此，有些方案提出使用 RSUs 作为群管理员[51,52]，但由于 RSUs 长期处于公共环境中，很容易遭到攻击与破坏。将 RSUs 作为群管理员，在实际中会给车辆的身份信息带来一定的风险。

第四类方案是基于对称密码学，这类方案是使用消息验证码（Message Authentication Code，MAC）来保障信息的完整性[46,53]。与公钥密码学最大的不同之处在于，对称密码学中签名与认证使用的密钥是相同的。虽然能够提高计算的效率，但却很难实现可追踪性。

最近几年出现了基于环签名的方案[54–56]，相比基于群签名的方案，环签名中因为没有群管理员的存在，相对来说更加安全。在这些方案中，车辆可以自由地生成签名，而不用依赖群管理员。由于环签名本身是一种完全匿名的签名方案，为了满足车辆的可追踪性，需要在环签名的方案上进行一些改进，将这种完全匿名变为有条件的匿名[57]。正因为没有了群管理员的控制，车辆可以自发产生一个基于某个环上的签名。但同时由于这种不可控制性，车辆生成的签名很可能是无效的。现有的基于环签名的方案都没有讨论如何确保环成员的有效性，因为缺少适当的验证操作，车辆很容易会产生一个无效的签名，这会给整个交通系统带来不确定

因素。

4.3 构造方案

通过前面的介绍，我们知道在车辆自组网中，车辆发送的消息一方面要能够被验证，另一方面要保证不泄漏隐私信息。看上去与基于属性的凭证中对属性的要求很类似。但二者之间也存在着很明显的差别。

在基于属性的凭证系统中，消息的有效性是靠凭证发行机构的签名保证的；而车辆自组网的环境中，车辆不能频繁地与 TRC 通信，因此信息的签名过程是由车辆自己完成的。那么，我们可不可以直接使用一种具有匿名性质的签名体制来同时保证匿名性和可验证性呢?

考虑到车辆自组网的特殊结构，环签名看上去是很不错的解决方案。但是环签名具备极高的自发性，如果车辆可以自由收集其他车辆的公钥并对消息进行签名的话，很容易由于环中存在失效的成员而使签名无效。现有的基于环签名的方案[54–56] 都没有考虑这个问题。在这些方案中，为了突出环签名的优势，直接移除了 RSUs，没有考虑 V2I 能发挥的作用。那么我们为什么不能将 RSUs 放到基于环签名的方案中呢? 如果可以将 RSUs 融入进去，并使用 V2I 的方式分配环成员，是不是就可以解决这个问题呢?

因此我们希望将 RSUs 与基于环签名的方案结合。在车辆进入某一区域时，需要通过向区域内的 RSUs 发出请求来获取一个成员列表。RSUs 在验证车辆的身份后，向其分配一个有效的成员列表。车辆收到这个列表后，便可以使用环签名的方式对需要发送的信息进行签名。

虽然环签名可以同时满足可验证性和匿名性这两个基本性质，但环签名带来的匿名是无条件的。因此我们签名上面附加一些可追踪的信息。以往的许多方案中，追踪这一功能是由 TRC 完成的，即 TRC 拥有权力可以直接根据生成的签名等信息还原出签名者的真实身份。但在实际中并不完全是这样，想象在出现交通事故时，一般是需要有执法部门完成对信息源的追踪，TRC 应该是起到辅助追踪的作用。因此我们引入了执法机关（Law Enforcement）这样一个实体，利用这种机构完成签名的追踪，并解析出签名者的假名。如果有进一步的需要，执法机关还可以根据这个假名从 TRC 的数据库中还原出其对应的真实 ID，并进行撤销操作。

要合理使用密码学的工具来构建这样一个方案不是容易的事情，一方面我们需要避开以前方案的劣势，另一方面我们需要在效率上满足一定的要求。这就需要与其它方案进行对比，还要找到合适的衡量方法体现方案高效率的特点。另外，在说明我们方案满足的性质的时候，需要对满足的这些性质进行合理的论证，有必

要的话还可以采取形式化的证明方式。为了方便证明，我们也可以引入随机预言机模型。在证明之前，通常需要引入合理的假设前提，并给出攻击者的攻击模型。

按照这样的思路，首先我们把车辆的假名从生成到撤销分为六个阶段，如图 4-2 所示。

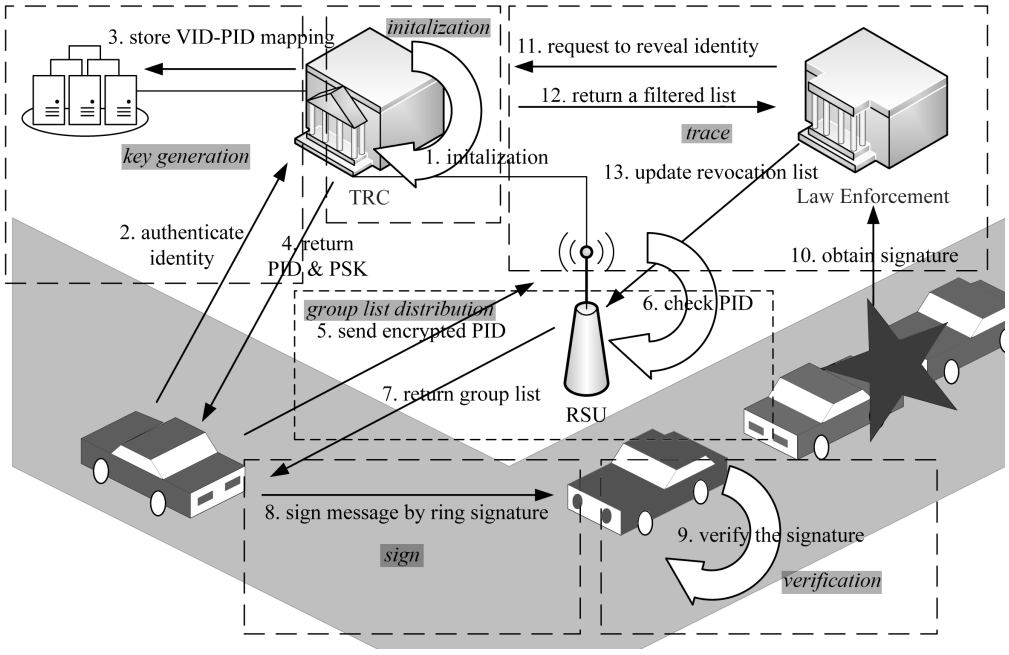

图 4-2 方案构造

从图中可以看到，在我们的方案中共有 4 类参与者，它们分别是交通管理中心（TRC），执法机关，配备了 OBUs 的车辆以及道路两旁的 RSUs。要把 RSUs 合理地融入到这个系统中不是一件容易的事。在充分考虑到 RSUs 特殊身份的情况下，我们提出使用基于身份的加密方案来完成车辆向 RSUs 的请求列表过程，利用对称密码机制完成 RSUs 的成员列表分配过程。根据双线性映射的性质，保证在一次交互之后，双方可以获得相同的密钥信息。为了完成追踪，我们在为签名的内容附加一个可追踪的 tag。为了方便说明，我们把需要使用的符号以及它所表示的含义列举出来，如表 4-2 所示。

具体的构造我们可以从初始化，密钥生成，成员列表分配，签名，验证和追踪这六个阶段详细地进行介绍。

4.3.1 初始化

系统的初始化过程包含一个 Setup 算法，这个算法是由 TRC 执行的。由于我们的方案是利用双线性映射来实现的，初始化的结果就是生成了一个双线性映射及相关的一些参数。

- $(pp, s) \leftarrow \mathrm{Setup}(1^{\kappa})$：在初始阶段，对于给定的安全参数 κ，算法 Setup$(\cdot)$

表 4-2 符号及其含义

符号	含义
s	TRC 的主私钥
PK	TRC 的公钥
s_{trac}	执法机关的私钥
PK_{trac}	执法机关的公钥
PP	公共参数
VID	OBUs 的真实 ID
PID	OBUs 的公钥（也称作假名）
PSK	OBUs 的私钥
RID	RSUs 的公钥
RSK	RSUs 的私钥
k_{i-j}	i 与 j 之间的共享公钥
L	成员列表，用于环签名
t_d	L 的失效时间
t	签名的时间戳
tag	用于追踪的标签
$a\|\|b$	将字符串 a 与 b 进行连接

可以生成公共参数 pp 和 TRC 的私钥 s。其中 $s \in_R \mathbb{Z}_q^*$ 是随机选取的，$pp = (\mathbb{G}_1, \mathbb{G}_T, P, q, e, PK, H_1, H_2)$。$\mathbb{G}_1$ 与 $\mathbb{G}_T$ 均为阶数为 q 的循环群，$e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$ 是一个双线性映射。P 是 $\mathbb{G}_1$ 的一个生成元，PK 又被称为 TRC 的公钥，且有 $PK = s \cdot P$。H_1 和 H_2 是两个密码哈希函数，且 $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$，$H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$。

在完成初始化过程之后，TRC 可以将 pp 进行公开，并保管好私钥 s。为了实现可追踪性，执法机关需要根据初始化后的公开参数 pp 生成对应的密钥对 (s_{trac}, PK_{trac})。其中 $s_{trac} \in_R \mathbb{Z}_q^*$，为执法机关的私钥，在进行追踪时会用到；$PK_{trac} = s_{trac} \cdot P$，作为执法机关的公钥，可以事先载入到车辆的 OBUs 设备中。

4.3.2 密钥生成

在初始化完成之后，RSUs 和配备有 OBUs 的车辆就可以从 TRC 处获取自己的密钥对。在这里我们需要做一个假设，即每辆车的 OBU 中都存在一个硬件安全模块（Hardware Security Module，HSM）[58]。存储在 HSM 中的信息不会遭到篡改，同时一些与密码学有关的操作如加密，签名等也是在 HSM 中完成。

系统中，每一辆车都有一个唯一的身份编号，我们用 VID 来表示。对于真实身份为 VID_ℓ 的车辆，它可以通过向 TRC 提交 VID_ℓ 来获取自己的密钥对。TRC 在收到 VID_ℓ 之后，开始执行 KeyGen(VID_ℓ) 算法，并把生成的密钥对及 pp 载入到 HSM 中。

- $(PID_\ell, PSK_\ell) \leftarrow \text{KeyGen}(VID_\ell)$：输出的 PID_ℓ 和 PSK_ℓ 分别代表着 VID_ℓ 的公钥和私钥。其中 $PID_\ell = H_1(VID_\ell || salt)$，$PSK_\ell = s \cdot PID_\ell$。$salt$ 是随机选取的，

即 $salt \in_R \mathbb{Z}_q^*$。为了实现可追踪性，执法机关的公钥 PK_{trac} 需要事先存储在 HSM 中。TRC 还会把 PID_ℓ 与 VID_ℓ 对应起来保存在数据库中。

类似地, 对于真实身份为 ID_j 的 RSU 来说, 它获取到的密钥对为 (RID_j, RSK_j), 其中 $RID_j = H_1(ID_j)$，$RSK_j = s \cdot RID_j$。与车辆编号 VID_ℓ 不同，RSU 的身份编号 ID_j 是可以直接公开的。因此对于车辆而言，某一区域内的 RSUs 信息均为可查的。

这里 RSUs 与 OBUs 获取假名的方式略有不同，OBUs 获取到的假名是在 VID 的基础上加盐哈希产生的，目的是车辆可以在不用更换 VID 的情况下可以从 TRC 处获取新的假名，满足车辆定期更换假名的需求。

由于 RSUs 是公共设施，而且 IDs 都是可以公开查询的，直接使用哈希获取假名的方式能够容易让其它车辆进行检验。即当车辆进入某一区域时，由于事先知道这一区域 RSUs 的 IDs，便可直接使用哈希函数 H_1 来计算 RSUs 的公钥（假名）。这样就可以使用此公钥进行数据的加密，从而避免出现与伪装成 RSUs 的设备进行通信的情况。

4.3.3 成员列表分配

当车辆进入一个区域时，它首先需要向该区域内的 RSUs 发送请求，在请求通过后，RSUs 再向其发送一个成员列表。为了方便说明，不妨假设车辆 VID_ℓ 在与 RSU_j 进行通信，在这一过程中，我们使用第二章 2.7 节中的基于身份的加密方案, 并使用 Enc 和 Dec 分别表示此方案的加密和解密算法[13]。另外, 我们使用 $\mathcal{ENC}(\cdot)$, $\mathcal{DEC}(\cdot)$，$\mathcal{HMAC}(\cdot)$ 分别表示对称密码体制下的加密算法、解密算法以及消息验证码算法。具体的通信过程可以分为以下几个步骤:

- RSU_j 在该区域内广播自己的公钥 PID_j;
- VID_ℓ 进入该区域后，首先可以获得 PID_j。由于 ID_j 是公开的，因此 VID_ℓ 可以直接用哈希算法判断 PID_j 的真实性。之后 VID_ℓ 就可以使用 PID_j 加密自己的假名，即 $C = \mathsf{Enc}(PID_\ell, RID_j)$，并把加密后的密文 C 发送给 RSU_j;
- RSU_j 在收到密文 C 之后后，可以利用自己的私钥计算出 VID_ℓ 的公钥，即 $PID_\ell = \mathsf{Dec}(C, RSK_j)$;
- RSU_j 开始检验 PID_ℓ 是否失效，如果已经失效，则直接拒绝 VID_ℓ 的请求，并终止与 VID_ℓ 的通信;
- 如果 PID_ℓ 是合法的，RSU_j 就可以计算共享密钥 $k_{j-\ell} = e(PID_\ell, RSK_j)$，并使用此密钥来加密群成员信息;
- RSU_j 选取一定的车辆公钥组成一个群成员列表 L，并使用对称密码学中的 Encrypt-then-MAC 的方法来传递 L，即先计算 $C^* = \mathcal{ENC}_{k_{j-\ell}}(L)$, 再计算 $\Sigma =$

$\mathcal{HMAC}_{k_{j-\ell}}(C^*||t_d)$，最后发送 (C^*, Σ, t_d) 给 VID_ℓ，其中 t_d 表示的是 L 的失效时间；

• VID_ℓ 在收到 RSU_j 发送的密文 C^* 后，首先计算它们之间的共享密钥 $k_{\ell-j} = e(PSK_\ell, RID_j)$，在消息认证码 Σ 通过验证后便可以还原出成员列表 $L = \mathcal{DEC}_{k_{i-j}}(C^*)$。

4.3.4 签名

在这里我们使用 Sign 与 Verify 分别表示前面介绍的基于身份的环签名的签名算法和验证算法。这两个算法的具体构造见第二章 2.8 节。

在拿到成员列表 L 之后，VID_ℓ 便可以使用 L 来完成环签名。对于 $L = \{PID_1, PID_2, ..., PID_n\}$ $(1 \le \ell \le n)$，这个过程由车辆 OBU 中的 HSM 完成。首先 HSM 会生成一个当前的时间戳 t，那么就可以计算可追踪的标签 tag：

$$tag = e(H_1(VID_\ell||t), PK_{trac}) \tag{4-1}$$

然后 VID_ℓ 可以使用第二章 2.8 节中介绍的环签名的方法生成对消息 m 的签名，即 $\sigma = \text{Sign}(m||t_d||tag||t, PSK_\ell, L)$，最后 VID_ℓ 广播 $(m, \sigma, L, t_d, t, tag)$。

4.3.5 验证

当车辆 VID_k 收到 $(m, \sigma, L, t_d, t, tag)$ 后，首先需要通过 t_d 判断 L 有没有失效。如果没有失效，VID_k 再执行验证算法 $\text{Verify}(m||t_d||tag||t, \sigma, L)$ 来验证 m 的有效性。

4.3.6 追踪

追踪是指当出现一些意外情况时，可以通过一些方法还原出签名者的真实身份。在过去提出的一些方案中，追踪是由 TRC 完成的，TRC 无疑拥有最高的权力。但在我们的方案中，要完成签名的追踪需要 TRC 与执法机关共同完成。追踪的过程主要依赖对 tag 中信息的分析。假设执法机关获取了 $tag = e(H_1(VID_\ell||t), PK_{trac})$ 后，首先它可以将 (L, t) 发送给 TRC，TRC 根据数据库中假名与车辆真实 VID 之间的对应关系找到相应的 VID_ℓ，也就是对于 $1 \le i \le n$，可以计算

$$H_i' = e(H_1(VID_i||t), P) \tag{4-2}$$

并把结果 $\{H_1', H_2', ..., H_n'\}$ 返回给执法机关。

执法机关在收到 $\{H_1', H_2', ..., H_n'\}$ 之后，首先利用自己的私钥将 tag 还原，即：

$$tag' = tag^{1/s_{trac}}$$

然后对 $\{H_1', H_2', ..., H_n'\}$ 中的每个成员与 tag' 进行比较，从中找出与 tag' 相等的 H'。那么被定位到的即为真正的签名者，执法机关可以根据此信息获取到签名者的假

名。需要进一步说明的是，根据假名信息，执法机关可以向 TRC 进行请求获得对应的真实 VID，如果该车辆需要被撤销，执法机关可以将其写入撤销列表。更新的撤销列表会同步到 RSUs 中，那么在之后的验证过程中，RSUs 将会直接拒绝该失效车辆的任何请求。

4.4 比较与分析

这一节主要是将我们的方案与其他方案进行对比分析。之前提出的一些基于公钥密码学和使用基于身份的密码学的方案都存在着假名更换的问题，由于我们的方案使用的采取的是环签名的机制，可以很好地避开这个问题。另外与其它环签名的方案相比，我们的方案能够很好地保障环成员列表可靠性。近些年，有一些使用了防篡改设备（Tamper-Proof Devices）在本地生成假名的方案[58–60]，我们在表 4-3 中列出了与这些方案的比较。

表 4-3 与其他方案的比较

	我们的方案	方案 I[59]	方案 II[58]	方案 III[60]
不可伪造性	√	√	√	√
可追踪	√	√	√	√
不可关联性	√	√	√	X
假名的可验证性	√	√	X	X
抗中间人攻击	√	√	√	√
抗重放攻击	√	√	√	√
假名（公钥）更换频率	低	高	高	高
对 RSU 的要求	半诚实	完全信任	完全信任	完全信任
完成追踪的实体	TRC 与执法机关合作	TRC	TRC	TRC

在对这些性质进行分析之前，我们先对车辆自组网中各个参与者建立如下的前提假设：

- 在这个系统中，TRC 与执法机关是完全可信的。由于 TRC 是整个系统的核心部分，车辆与 RSU 的密钥都是依赖它分配的。执法机关只有在需要追溯恶意的签名者时才会去向 TRC 发送追踪请求。并且我们假设他们之间不会共谋；
- RSUs 在这个系统中可以看做不完全受信任的（Semi-Trusted），这意味着 RSUs 会正常执行系统的协议，但可能会尝试去分析车辆发送的信息。换句话说，RSUs 在分配成员列表的过程中，不会去修改需要发送的信息，但可能通过分析车辆发送的信息尝试还原车辆的真实身份；
- 系统中的车辆可以修改通信的数据信息，但一些保存在 HSM 中的参数是不可修改的且不会外泄的。且在 HSM 中进行的操作我们都可以认为是安全的；
- 系统中的通信环境是不安全的，攻击者可以窃听并修改通信过程中的数据

信息，或者直接伪造虚假信息来破坏系统的安全性。

对于硬件安全模块 HSM，我们可以将其看做由 5 个不同功能的子模块组成，这 5 个模块分别为假名校验模块，加密模块，解密模块，签名模块和验证模块。这些模块可以通过一定的输入来得到相应的输出结果。它们的组成如图 4-3 所示。

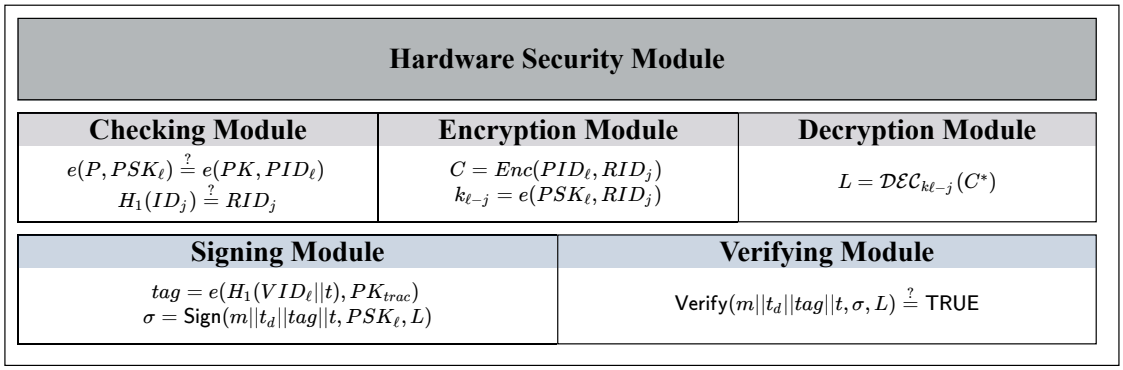

图 4-3 组成 HSM 的各个模块

当 TRC 完成初始化工作之后，生成的公共参数 $pp = (\mathbb{G}_1, \mathbb{G}_2, P, q, e, PK, H_1, H_2)$ 被预先载入到 HSM 模块中。从图中可以看出，当车辆 V_ℓ 获取到自己的密钥对 (PID_ℓ, PSK_ℓ) 并将密钥对载入到 HSM 中时，HSM 中的假名校验模块首先对这对密钥进行校验。校验的过程就是检查以下等式是否成立：

$$e(P, PSK_\ell) \stackrel{?}{=} e(PK, PID_\ell) \tag{4-3}$$

如果校验通过，那么 HSM 就可以载入这对密钥以进行后面的操作。

在成员列表分配阶段，车辆 V_ℓ 在收到 RSU_j 的公钥 PID_j 之后，首先需要调用 HSM 的假名校验模块来校验 RSU_j 的公钥 PID_j 是否合法。由于不同区域内的 RSUs 身份信息 ID_j 都是公开可查的，通过提供 PID_j 和 ID_j 给 HSM，HSM 只需要检查以下等式是否成立：

$$H_1(ID_j) \stackrel{?}{=} RID_j \tag{4-4}$$

如果校验通过，HSM 中的加密模块便自动使用 RID_j 作为加密的公钥对车辆的假名 PID_ℓ 进行加密。即计算：

$$C = \mathsf{Enc}(PID_\ell, RID_j) = (rP, PID_\ell \oplus g_d^r) \tag{4-5}$$

其中，$g_d^r = e(PID_\ell, PK)$。

在输入加密的密文之后，HSM 还需要计算与 RSU_j 对应的共享密钥，即计算：

$$k_{\ell-j} = e(PSK_\ell, RID_j) \tag{4-6}$$

并把此共享密钥作为解密模块的解密密钥。

在收到 RSU_j 返回的 (C^*, Σ, t_d) 之后，HSM 的解密模块开始验证 t_d 是否失效，如果还未失效则再验证消息验证码 Σ。在这些都通过验证之后，便可以使用对称解密算法 $\mathcal{DEC}_{k_{\ell-j}}(C^*)$ 对密文 C^* 进行解密。值得注意的是，在实际应用中，我们可以使用 AES 作为对称加解密算法，这类算法现在已经很成熟，计算效率比较高。

在完成了对成员列表的还原之后，签名模块便可以使用此列表 L 作为输入，并输出对消息 m 的一个环签名。验证模块则是在收到其它车辆的签名信息后，利用验证算法 Verify 完成对消息 m 的验证。

下面我们将对此方案满足的可验证性、匿名性、不可伪造性、可追踪性、抗重放攻击以及高效性分别进行说明。为了方便描述，我们依然使用 V_ℓ 代表进行签名的车辆，用 V_k 表示验证签名的车辆。

4.4.1 可验证性

可验证性指的是，在此方案中如果所有过程都是正确执行的，那么最终得到的签名一定可以通过验证。因此我们需要考虑成员列表分配过程以及签名和验证过程的正确性。从前面的描述我们可以知道，V_ℓ 在向 RSU_j 请求成员列表时，发送给 RSU_j 的密文是：

$$C = (rP, V) = (rP, PID_\ell \oplus g_d^r) \tag{4-7}$$

RSU_j 在收到此密文后，计算 $V \oplus e(RSK_j, rP)$，由于：

$$V \oplus e(RSK_j, rP) = V \oplus e(RID_j, s \cdot P)^r = V \oplus g_d^r = PID_\ell \tag{4-8}$$

因此 RSU_j 能够正确获取车辆 V_ℓ 的假名 PID_ℓ。而 RSU_j 计算的共享秘钥为 $k_{j-\ell} = e(PID_\ell, RSK_j)$，$VID_\ell$ 计算的共享秘钥为 $k_{\ell-j} = e(PSK_\ell, RID_j)$，由双线性映射的性质可以得到：

$$e(PID_\ell, RSK_j) = e(PID_\ell, s \cdot RID_j) = e(s \cdot PID_\ell, RID_j) = e(PSK_\ell, RID_j) \tag{4-9}$$

双方在这个交互过程中获取了相同的密钥，再根据对称密码体制的特点，从而保证 V_ℓ 可以从 RSU_j 处正确获取成员列表信息。

对于车辆 V_ℓ 以及成员列表 $L = \{PID_1, PID_2, ..., PID_n\}$ $(1 \le \ell \le n)$，以及所需签名的信息 m，我们可以令 $m' = m||t_d||tag||t$。那么通过得到的签名 σ 为：

$$\sigma = (\cup_{i=1}^{n}\{U_i\}, V) \tag{4-10}$$

其中，对于 $1 \le i \le n$ 且 $i \ne \ell$，U_i 都是从 $\mathbb{G}_1$ 中随机选取的，我们记 $h_i = H_2(m'||L||U_i)$。

计算完成后我们可以随机选取 $r'_\ell \in_R \mathbb{Z}_q^*$，并计算 $U_\ell = r'_\ell PID_\ell - \sum_{i\neq\ell}\{U_i + h_i PID_i\}$，$h_\ell = H_2(m'||L||U_\ell)$。最后可得到 $V = (h_\ell + r'_\ell)PSK_\ell$。

在验证的过程中，对于 $1 \leq i \leq n$，车辆 V_k 首先计算 $h_\ell = H_2(m'||L||U_i)$，那么根据双线性映射的性质，我们可以得到下面的等式：

$$\begin{aligned} e(PK, \sum_{i=1}^{n}(U_i + h_i PID_i)) =& e(s\cdot P, U_\ell + h_\ell PID_\ell + \sum_{i=1,i\neq\ell}^{n}(U_i + h_i PID_i)) \\ =& e(s\cdot P, r'_\ell PID_\ell + h_\ell PID_\ell) \\ =& e(s\cdot P, (r'_\ell + h_\ell)PID_\ell) \\ =& e(P, (r'_\ell + h_\ell)PID_\ell \cdot s) \\ =& e(P, V) \end{aligned} \tag{4-11}$$

因此，只要 V_ℓ 正确执行相关的协议，那么产生的签名一定能够通过 V_k 的验证。

4.4.2 匿名性

我们主要从 V2I 和 V2V 两个角度分析匿名性，从 V2I 的角度，由于 RSU_j 是半诚实的，在与车辆 V_ℓ 的通信过程中，它唯一知道的就是车辆 V_ℓ 的公钥，即 PID_ℓ。由于 PID_ℓ 是由 TRC 生成的，且 $PID_\ell = H_1(VID_\ell||salt)$。根据密码哈希函数的单向性，在只知道 PID_ℓ 的情况下，RSU_j 能在概率概率多项式时间内找到一个 ID 使得 $H_1(ID) = PID_\ell$ 的概率是可以忽略不计的。而且我们建议车辆的公钥需要定时更新，由此保证了 RSU_j 无法将 PID_ℓ 与车辆的真实身份关联起来。

从 V2V 的角度，由于我们选择的是由 Chow，Yiu 和 Hui 提出的基于身份的环签名方案，这种环签名方案具有完全的匿名性，因此在知道车辆 V_ℓ 生成的签名 σ 的情况下，车辆 V_k 根据列表 L 只能推断出签名者在列表 L 内这条信息，并不能推断出签名者具体是列表中的哪一位。这样就能够很好地保证签名者的匿名性。另外，在广播的信息中还存在可追踪的标签，即 $tag = e(H_1(VID_\ell||t), PK_{trac})$。密码哈希函数的性质保证了车辆 V_k 不能根据 tag 的值从中获取到有用的信息。

4.4.3 不可伪造性

在前面的假设中，我们假定 RSUs 是不完全受信任的，也就是说 RSUs 不会篡改或伪造数据，因此我们在考虑不可伪造性时，只需要考虑系统中的恶意车辆。与前面分析类似，我们分别从 V2I 与 V2V 两个方面进行说明。

在 V2I 的过程中，假设有一恶意的车辆 $VID_{i'}$ 想伪装成 VID_ℓ 并与 RSU_j 进行通信。假设 $VID_{i'}$ 已经知道了 VID_ℓ 的公钥为 PID_ℓ，那么 RSU_j 向他返回的就是用 $k_{j-\ell}$ 加密的信息。由于我们使用的是对称密码体制，并且采用 Encrypt-then-MAC

的模式。这种模式是满足选择密文安全的，也就是说 $V_{i'}$ 在没有密钥 $k_{j-\ell}$ 的情况下不能获取到任何有用的信息。因此我们只需要证明 $V_{i'}$ 在只知道 PID_ℓ 的情况下对它获取到密钥 $k_{j-\ell}$ 没有任何帮助。下面我们使用基于游戏（Game-Based）的方式进行证明。

假设挑战者 C_1 与攻击者 $V_{i'}$ 进行下面这个游戏 $Game_1$：

1. 挑战者 C_1 生成参数 $pp = (\mathbb{G}_1, \mathbb{G}_T, P, q, e, PK, H_1)$ 和主密钥 s，并随机挑选两个 ID：$ID_1 \in_R \mathbb{Z}_q^*$，$ID_2 \in_R \mathbb{Z}_q^*$，令 $PID_\ell := H_1(ID_1), RID_j := H_1(ID_2)$。最后将 (pp, PID_ℓ, RID_j) 发送给攻击者 $V_{i'}$；

2. 挑战者 C_1 选择一个比特 $b \in_R \{0,1\}$，如果 $b = 0$，则令 $h := k_{j-\ell}$；如果 $b = 1$，则随机选取 $h \in_R \mathbb{G}_T$。挑战者将 h 发送给攻击者 $V_{i'}$；

3. 攻击者收到 h 之后，在多项式时间内返回一个比特 b'；

4. 挑战者 C_1 判断 b' 是否等于 b，若 $b' = b$，则称攻击者 $V_{i'}$ 成功；如果 $b' \neq b$，则称其攻击失败。

在进行多项式次数后，我们用 $\Pr[\mathsf{Game}_1(V_{i'}) = 1]$ 表示攻击者 $V_{i'}$ 在 $Game_1$ 中获胜的概率。

类似地，我们假设有挑战者 C_2 与攻击者 $\mathcal{A}$ 进行下面的游戏 $Game_2$：

1. 挑战者 C_2 生成参数 $pp = (\mathbb{G}_1, \mathbb{G}_T, P, q, e, PK, H_1)$ 和主私钥 s，并随机选取 $a \in_R \mathbb{Z}_q^*, b \in_R \mathbb{Z}_q^*$，令 $y_1 = a \cdot P, y_2 = b \cdot P$。最后将 (pp, y_1, y_2) 发送给攻击者 $\mathcal{A}$；

2. 挑战者 C_2 选择一个比特 $b \in_R \{0,1\}$，如果 $b = 0$，则令 $h := e(y_1, y_2)^s$；如果 $b = 1$，则随机选取 $h \in_R \mathbb{G}_T$。C_2 将 h 发送给攻击者 $\mathcal{A}$；

3. 攻击者 $\mathcal{A}$ 接收到 h 后，在多项式时间内返回一个比特 b'；

4. 挑战者 C_2 判断 b' 是否与 b 相等，若 $b' = b$，则称攻击者 $\mathcal{A}$ 攻击成功；否则称 $\mathcal{A}$ 攻击失败。

在进行多项式次数后，我们用 $\Pr[\mathsf{Game}_2(\mathcal{A}) = 1]$ 表示攻击者 $\mathcal{A}$ 在 $Game_2$ 中获胜的概率。

由 DBDH 问题的定义，我们把在 $Game_2$ 中获胜看做解决一个 DBDH 问题。由于我们假设 DBDH 问题是一个困难问题，那么存在一个可忽略函数 $\mathsf{negl}(\kappa)$，使得：

$$|\Pr[\mathsf{Game}_2(\mathcal{A}) = 1] - \frac{1}{2}| \leq \mathsf{negl}_1(\kappa) \tag{4-12}$$

始终成立。

由于 H_1 是一个 Map-to-Point 的密码哈希函数，在随机预言机模型的假设下，我们可以得到：

$$|\Pr[\mathsf{Game}_1(V_{i'})=1]-\Pr[\mathsf{Game}_2(\mathcal{A})=1]|\le \mathsf{negl}_2(\kappa) \tag{4-13}$$

由公式（4-12）与（4-13），我们可以推出：

$$|\Pr[\mathsf{Game}_1(V_{i'})=1]-\frac{1}{2}|\le \mathsf{negl}_1(\kappa)+\mathsf{negl}_2(\kappa) \tag{4-14}$$

也就是说，$V_{i'}$ 在 $Game_1$ 中能取得成功的概率与随机选取一个比特的概率是基本相同的。即在随机预言机模型的假设下，$V_{i'}$ 在只知道 PID_ℓ 与 RID_j 的情况下无法获取到共享秘钥 $k_{j-\ell}$ 的任何信息。

在 V2V 的过程中，签名 σ 是由 HSM 计算并输出的，签名的内容是 $m||t_d||tag||t$。由于我们使用的签名方案具有适应性选择消息和身份下的存在性不可伪造的特性，因此恶意的车辆 $V_{i'}$ 对 (t_d,tag,t,L) 中任一内容进行伪造都将通过不了验证。

4.4.4 可追踪性

在一些特殊情况下，如出现意外事故的情况下，执法机关将有必要调查事故中信息的真正签名者。假设车辆 $V_{i'}$ 发送的消息为 m，对应的签名为 σ。我们知道，车辆 $V_{i'}$ 发送的信息中还包括一个可追踪的 tag，且

$$tag=e(H_1(VID_{i'}||t),PK_{trac}) \tag{4-15}$$

执法机关首先将 (L,t) 提交给 TRC，其中 $L=\{PID_1,PID_2,...,PID_n\}(1\le i'\le n)$。之后计算 tag'，即：

$$tag'=tag^{1/s_{trac}}=e(H_1(VID_{i'}||t),s_{trac}^{-1}PK_{trac})=e(H_1(VID_{i'}||t),P) \tag{4-16}$$

而 TRC 返回的为一个列表，即：

$$L'=\{e(H_1(VID_1||t),P),e(H_1(VID_2||t),P),...,e(H_1(VID_n||t),P)\} \tag{4-17}$$

由于 $1\le i'\le n$，因此 tag' 一定属于列表 L'，那么也就是说一定可以根据 tag' 和 L' 来判断出签名者的假名 $PID_{i'}$。在找到 $PID_{i'}$ 之后，执法机关也可以进一步通过向 TRC 发出请求还原出 $PID_{i'}$ 对应的真实身份 $VID_{i'}$，并完成撤销等一系列操作。因为 tag 的不可伪造性（根据前面的论述以及 HSM 的特性），通过这个过程一定可以找到真正的签名者，而且所需要的时间与 L 的长度成正比。

对于 TRC 来说，它在不知道 tag 的情况下，仅仅根据执法机关递交的 (L,t) 的信息无法判断出执法机关所需要还原的签名者的身份。执法机关只有在真正确定该车辆为恶意车辆的情况下，才会向 TRC 请求还原其真实的身份，从某种意义上来说也是避免了在未真正确定事故真相之前过早暴露车辆身份。

4.4.5 抗重放攻击

重放攻击（Replay Attack）指的是恶意用户通过收集合法有效的数据信息并加以重复使用以达到伪装成真实用户的目的。一般我们使用添加时间戳的方法阻止网络环境中的重放攻击。由于车辆自组网处在一个公开的网络环境中，车辆之间发送的信息大多以广播的形式传送，因此很容易被其它恶意的用户或车辆进行收集。不附加时间戳的话，车辆发送的信息很方便被其它网络节点利用。

在我们的方案中，假设恶意车辆 $V_{i'}$ 在收到了广播信息 (m,σ,L,t_d,t,tag) 之后，尝试再隔一段时间重复广播此信息。由于广播信息中包含了签名时生成的时间戳 t，如果 $V_{i'}$ 不做任何修改直接发送信息 (m,σ,L,t_d,t,tag) 的话，则会因为当前时间与 t 相差太大而通不过其它车辆的校验；如果 $V_{i'}$ 尝试修改 t 为当前时间，又因为 $\sigma = \mathsf{Sign}(m||t_d||t||tag||t,PSK_\ell,L)$，也会通不过其它车辆的验证。因此，在这种对实时性要求比较高的车辆自组网环境中，t 的存在一方面可以确保消息 m 的时效性，另一方面可以防御重放攻击。要能有效地抵抗重放攻击，一个比较重要的条件是车辆自组网中的设备需要准确的时间同步。

4.4.6 高效性

由于我们的方案是在双线性映射上进行的，首先我们需要对双线性映射上相关操作的运算时间进行估算。下面的测试是在搭载英特尔酷睿 i7-6700 处理器的 Linux 64 位系统环境中进行的，调用的是基于 Python 语言的 CHARM 库[61]。特别地，我们使用的是 512 位椭圆曲线，对其上面的每个操作分别进行了 10000 次随机运算，并将运行消耗的 CPU 时间取平均值。最终我们把比较耗时的运算列举出来，如表 4-4 所示。

表 4-4 双线性映射上单个操作的运算耗时

符号	描述	CPU 时间（单位：ms）
T_{bp}	执行一次双线性映射计算的时间	0.718
T_{ep}	对 $\mathbb{G}_T$ 中的元素执行一次指数运算所需的时间	1.228
T_{em}	对 $\mathbb{G}_1$ 上的点执行一次标量乘法所需的时间	1.245
T_{mph}	执行一次 Map-to-Point 哈希函数所需的时间	2.606

其他的操作，如椭圆曲线上的加法，哈希函数 H_2，对称加密解密算法及 MAC 运算所需时间较短，相较上表中的可以忽略不计。我们用 n 来表示环签名中列表成员的数量，当 $n = 10$ 的情况下，各个阶段所需要花费的时间如表 4-5 所示。

从表中我们可以看到，主要是签名和验证的过程花费的时间比较长，且消耗的时间与使用的列表长度成正比。因此，需要进一步对比近些年其他基于环签名的方案中[55,56] 签名和验证所需要的时间。如表 4-6 所示，我们列举了在签名以及

表 4-5 方案中各个阶段所需时间（单位：ms）

	TRC	RSU	OBU
初始化：	$T_{em} \approx 1.245$	-	-
密钥生成：	$T_{mph} + T_{em} \approx 3.851$	-	-
列表分发：	-	$T_{bp} \approx 0.718$	$2T_{bp} + T_{ep} \approx 2.664$
签名：	-	-	$(n+1)T_{em} + T_{bp} \approx 14.940$
验证：	-	-	$2T_{bp} + nT_{em} \approx 15.131$

验证两个方面与其他基于环签名的方案的对比。

表 4-6 与其他基于环签名的方案的对比（单位：ms）

	签名所需时间	验证所需时间
方案 IV[55]	$2T_{bp} + 2T_{ep} + (2n+2)T_{em} \approx 31.282$	$T_{bp} + 2(n+1)T_{ep} \approx 26.506$
方案 V[56]	$3T_{bp} + 4T_{ep} + 2nT_{em} + 2T_{mph} \approx 37.178$	$3T_{bp} + 3T_{ep} + (n+2)T_{em} \approx 20.778$
我们的方案	$(n+1)T_{em} + T_{bp} \approx 14.940$	$2T_{bp} + nT_{em} \approx 15.131$

通过对比我们发现，该方案在签名方面所需的时间要明显低于另外两个方案。在实际生活场景中，车辆自组网的通信主要依赖于 DSRC（Dedicated Short-Range Communication）技术。该技术基于 IEEE 802.11p 标准，能够很好地支持车辆间的无线通信。DSRC 技术中规定信息发送的频率为 1-10HZ[46]，而我们方案中毫秒级的签名与验证速度已经可以满足在车辆自组网中对效率的要求。

4.5 本章小结

这一章我们首先介绍了车辆自组网的概念，并分析了在车辆自组网的环境中存在的安全与隐私方面的问题。在给出提出的方案之前，我们整理了已有的一些解决方案，并说明了这些方案存在的问题。通过与基于属性的凭证系统的对比，我们决定使用具有匿名性质的签名方案来构造一个功能完备的方案。尽管我们也是使用环签名的方法来保证车辆通信过程中消息的可验证性及车辆身份的匿名性，但我们的方案充分发挥了 RSUs 的作用，并利用 RSUs 保证了签名的可靠性。为了将 RSUs 很好地融入到车辆自组网的环境中，我们结合了基于身份的密码学以及对称密码体制的优势，从而在保证效率的同时满足了车辆自组网中的需求。为了很好地进行说明，我们将车辆网中参与交互的实体分为了 TRC、执法机关、配备了 OBUs 的车辆和固定区域内的 RSUs 这四类。它们分别执行不同的功能。TRC 负责系统参数的生成和假名的生成，RSUs 负责向该区域内的车辆分配成员列表，车辆在获取到列表后便可以使用环签名的方式完成信息的签名与认证。执法机关与 TRC 合作可以还原出签名者的真实身份。

我们的方案与其它方案相比最大的优势是车辆不用频繁地更换自己的假名，在追踪的过程中引入了执法机关，并且只有在执法机关与 TRC 合作的情况下才能还

原签名者的真实身份。这样的做法比较符合实际中的场景，同时也在最大程度上保护了用户的隐私。

在这一章的最后，通过与其它基于环签名的方案进行对比可以看到，我们方案的计算量相对较低，因此能够用在车辆自组网这种对实时性要求比较高的场景中。

结　论

在研究基于属性的凭证系统的过程中，我们了解到许多解决隐私保护问题的方法。这些方法与现代密码学紧密相连。在现代密码学中有许多有用的工具，如数字签名、零知识证明、承诺机制等等，通过将这些工具结合起来，我们可以解决实际生活中的具体问题。

实际生活中有很多亟待解决的安全与隐私问题，基于属性的凭证就是用于解决用户在进行身份认证的场景下的隐私保护问题。我们详细介绍了基于属性的凭证的由来以及它的发展过程，通过调研大量的文献资料，我们对匿名凭证需要满足的性质进行了总结，并对匿名凭证系统中各个角色的交互过程进行了归纳。通过对现有的匿名凭证系统如 IdeMix、U-Prove 和 ABC4Trust 等的探讨，我们概括了匿名凭证系统的发展规律，并逐步理解构造基于属性凭证背后所用到的密码学思想。

沿着这条思路，我们开始寻找相关的应用场景。通过对车辆自组网环境的充分调研，我们发现了其中存在的隐私与安全问题。目前这些问题还没有很好的解决方案，因此我们决定利用基于属性的凭证的思想来对这个问题进行深入的研究。

以往的解决方案中，车辆需要频繁地更换自己的假名以达到匿名的目的。假名的生成方式要么由 TRC 完成，要么由车辆自己生成。这种频繁更换的方式还不能真正意义上地阻止对身份的追踪，因此一些基于特殊性质的签名方案（如群签名、环签名）的解决方法开始被提出。

我们的方案也是基于环签名的，这样最大的好处是增加了假名的利用率，减少了更换假名的频率。但与其它基于环签名方案最大的不同点在于，其它基于环签名的方案中没有考虑到成员的有效性问题，由于环签名本身的高自由度，这样生成的签名很有可能是失效的。

因此，我们通过基于身份的密码体制，将 RSUs 很好地融入到系统中来，充当分配成员列表的角色。最终我们提出了一个结合了多个密码体制的方案。此方案主要有以下几个特点：

1. 缩减了更换假名的频率，从而避免因为频繁更换假名带来的计算和存储瓶颈；

2. 提出了一个高效的密钥分配方案，只需要一次交互便可以完成通信双方的密钥协商，并利用对称加密机制完成数据的通信；

3. 利用执法机关与 TRC 合作还原出签名者的真实身份，这样的做法有利于维

护签名者的隐私，更符合现实生活中的实际应用场景。

由于我们使用的是比较轻量级的加密与签名方案，因此在效率方面要比其他基于环签名的方案高。我们对方案中所实现的性质进行了充分的证明，即在配备有安全模块 HSM 的假设前提下，我们提出的方案具备可验证性、匿名性和可追踪性等基本性质，并且我们还证明在随机预言机模型下具备不可伪造性。

除了这些优势之外，我们方案还有许多需要完善的地方。比如在安全性上要依赖 HSM，我们应该考虑在没有 HSM 的场景中如何确保能满足这些性质。而在随机预言机模型下的安全性证明只能表明系统在某种意义上是安全的，还可以考虑在没有随机预言机的情况下完成安全性证明。在进行撤销方面，我们没有进行太多的讨论，或许可以尝试使用基于累加器的方法来提高撤销的效率。在最后的效率分析中，我们缺少更有说服力的仿真测试，这些都是需要我们将来进一步完成的。

参考文献

[1] Camenisch J, Van Herreweghen E. Design and implementation of the idemix anonymous credential system[C] // Proceedings of the 9th ACM conference on Computer and communications security. 2002 : 21 – 30.

[2] Sabouri A, Krontiris I, Rannenberg K. Attribute-based credentials for trust (ABC4Trust)[C] // International Conference on Trust, Privacy and Security in Digital Business. 2012 : 218 – 219.

[3] Vullers P, Alpár G. Efficient selective disclosure on smart cards using idemix[C] // IFIP Working Conference on Policies and Research in Identity Management. 2013 : 53 – 67.

[4] Garman C, Green M, Miers I. Decentralized Anonymous Credentials.[C] // NDSS. 2014.

[5] Blömer J, Bobolz J. Delegatable attribute-based anonymous credentials from dynamically malleable signatures[C] // International Conference on Applied Cryptography and Network Security. 2018 : 221 – 239.

[6] De Fuentes J M, González-Manzano L, Serna-Olvera J, et al. Assessment of attribute-based credentials for privacy-preserving road traffic services in smart cities[J]. Personal and Ubiquitous Computing, 2017, 21(5) : 869 – 891.

[7] Neven G, Baldini G, Camenisch J, et al. Privacy-preserving attribute-based credentials in cooperative intelligent transport systems[C] // 2017 IEEE Vehicular Networking Conference (VNC). 2017 : 131 – 138.

[8] Viejo A, Sánchez D. Secure and privacy-preserving orchestration and delivery of fog-enabled IoT services[J]. Ad Hoc Networks, 2019, 82 : 113 – 125.

[9] 张严, 张立武. 匿名凭证方案研究进展 [J]. 信息网络安全, 2012(1) : 0 – 0.

[10] 胡江红, 杜红珍, 张建中. 可证明安全的基于证书聚合签名方案 [J]. 数学的实践与认识, 2017, 47(3) : 128 – 135.

[11] 柳欣, 张波. 基于 DAA-A 的改进可授权电子现金系统 [J]. 计算机研究与发展, 2016, 53(10) : 2411 – 2428.

[12] 柳欣, 徐秋亮, 张波. 基于 DAA 的轻量级多商家多重息票系统 [J]. 通信学报, 2016, 37(9) : 30 – 45.

[13] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C] // Annual International Cryptology Conference. 2001 : 213 – 229.

[14] Chow S S, Yiu S-M, Hui L C. Efficient identity based ring signature[C] // International Conference on Applied Cryptography and Network Security. 2005 : 499 – 512.

[15] Krawczyk H. The order of encryption and authentication for protecting communications (or: How secure is SSL?)[C] // Annual International Cryptology Conference. 2001 : 310 – 331.

[16] 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.

[17] 张方国. 从双线性对到多线性映射 [J]. 密码学报, 2016, 3(3) : 211 – 228.

[18] Joux A. A one round protocol for tripartite Diffie–Hellman[C] // International Algorithmic Number Theory Symposium. 2000 : 385 – 393.

[19] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols[C] // Proceedings of the 1st ACM Conference on Computer and Communications Security. 1993 : 62 – 73.

[20] Koblitz N, Menezes A J. The random oracle model: a twenty-year retrospective[J]. Designs, Codes and Cryptography, 2015, 77(2-3) : 587 – 610.

[21] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems[J]. SIAM Journal on Computing, 1989, 18(1) : 186 – 208.

[22] Camenisch J, Stadler M. Efficient group signature schemes for large groups[C] // Annual International Cryptology Conference. 1997 : 410 – 424.

[23] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems[C] // Conference on the Theory and Application of Cryptographic Techniques. 1986 : 186 – 194.

[24] Shamir A. Identity-based cryptosystems and signature schemes[C] // Workshop on the Theory and Application of Cryptographic Techniques. 1984 : 47 – 53.

[25] Rivest R L, Shamir A, Tauman Y. How to leak a secret[C] // International Conference on the Theory and Application of Cryptology and Information Security. 2001 : 552 – 565.

[26] Chaum D, Van Heyst E. Group signatures[C] // Workshop on the Theory and Application of of Cryptographic Techniques. 1991 : 257 – 265.

[27] Chaum D. Security without identification: Transaction systems to make big brother obsolete[J]. Communications of the ACM, 1985, 28(10) : 1030 – 1044.

[28] Chaum D, Evertse J-H. A secure and privacy-protecting protocol for transmitting personal information between organizations[C] // Conference on the Theory and Application of Cryptographic Techniques. 1986 : 118 – 167.

[29] Camenisch J, Lysyanskaya A. An efficient system for non-transferable anonymous credentials with optional anonymity revocation[C] // International Conference on the Theory and Applications of Cryptographic Techniques. 2001 : 93 – 118.

[30] Chen L. Access with pseudonyms[C] // Cryptography: Policy and Algorithms. 1996 : 232 – 243.

[31] Lysyanskaya A, Rivest R L, Sahai A, et al. Pseudonym systems[C] // International Workshop on Selected Areas in Cryptography. 1999 : 184 – 199.

[32] Brands S. Rethinking public key infrastructures and digital certificates building in privacy[J], 1999.

[33] Paquin C, Zaverucha G. U-prove cryptographic specification v1. 1[J]. Technical Report, Microsoft Corporation, 2011.

[34] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing[C] // International Conference on the Theory and Application of Cryptology and Information Security. 2001 : 514 – 532.

[35] Camenisch J, Lysyanskaya A. Signature schemes and anonymous credentials from bilinear maps[C] // Annual International Cryptology Conference. 2004 : 56 – 72.

[36] Okamoto T. Efficient blind and partially blind signatures without random oracles[C] // Theory of Cryptography Conference. 2006 : 80 – 99.

[37] Blanton M. Online subscriptions with anonymous access[C] // Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. 2008 : 217 – 227.

[38] Akagi N, Manabe Y, Okamoto T. An efficient anonymous credential system[C] // International Conference on Financial Cryptography and Data Security. 2008 : 272 – 286.

[39] Groth J, Sahai A. Efficient non-interactive proof systems for bilinear groups[C] // Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2008 : 415 – 432.

[40] Belenkiy M, Chase M, Kohlweiss M, et al. P-signatures and noninteractive anonymous credentials[C] // Theory of Cryptography Conference. 2008 : 356 – 374.

[41] Belenkiy M, Camenisch J, Chase M, et al. Randomizable proofs and delegatable anonymous credentials[C] // Advances in Cryptology-CRYPTO 2009. [S.l.] : Springer, 2009 : 108 – 125.

[42] Camenisch J, Kohlweiss M, Soriente C. An accumulator based on bilinear maps and efficient revocation for anonymous credentials[C] // International Workshop on Public Key Cryptography. 2009 : 481 – 500.

[43] Fuchsbauer G, Hanser C, Slamanig D. Structure-preserving signatures on equivalence classes and constant-size anonymous credentials[J]. Journal of Cryptology, 2018 : 1 – 49.

[44] Bichsel P, Camenisch J, Groß T, et al. Anonymous credentials on a standard java card[C] // Proceedings of the 16th ACM conference on Computer and communications security. 2009 : 600 – 610.

[45] El Zarki M, Mehrotra S, Tsudik G, et al. Security issues in a future vehicular network[C] // European Wireless : Vol 2. 2002.

[46] Petit J, Schaub F, Feiri M, et al. Pseudonym schemes in vehicular networks: A survey[J]. IEEE communications surveys & tutorials, 2015, 17(1) : 228 – 255.

[47] Wiedersheim B, Ma Z, Kargl F, et al. Privacy in inter-vehicular networks: Why simple pseudonym change is not enough[C] // 2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS). 2010 : 176 – 183.

[48] Jemaa I B, Kaiser A, Lonc B. Study of the impact of pseudonym change mechanisms on vehicular safety[C] // Vehicular Networking Conference (VNC), 2017 IEEE. 2017 : 259 – 262.

[49] Ying B, Makrakis D, Mouftah H T. Dynamic mix-zone for location privacy in vehicular networks[J]. IEEE Communications Letters, 2013, 17(8) : 1524 – 1527.

[50] Lu R, Lin X, Luan T H, et al. Pseudonym changing at social spots: An effective strategy for location privacy in vanets[J]. IEEE Transactions on Vehicular Technology, 2012, 61(1) : 86 – 96.

[51] Hao Y, Cheng Y, Zhou C, et al. A distributed key management framework with cooperative message authentication in VANETs[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(3) : 616 – 629.

[52] Park M-H, Gwon G-P, Seo S-W, et al. RSU-based distributed key management (RDKM) for secure vehicular multicast communications[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(3) : 644 – 658.

[53] Choi J Y, Jakobsson M, Wetzel S. Balancing auditability and privacy in vehicular networks[C] // Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks. 2005 : 79 – 87.

[54] Xiong H, Beznosov K, Qin Z, et al. Efficient and spontaneous privacy-preserving protocol for secure vehicular communication[C] // 2010 IEEE International Conference on Communications. 2010 : 1 – 6.

[55] Chaurasia B K, Verma S. Conditional Privacy through Ring Signature in Vehicular Ad-hoc Networks[J]. Transactions on Computational Science XIII, 2011, 6750 : 147.

[56] Zeng S, Huang Y, Liu X. Privacy-preserving communication for VANETs with conditionally anonymous ring signature[J]. International Journal of Network Security, 2015, 17(2) : 135 – 141.

[57] 张建明, 赵玉娟, 江浩斌, et al. 车辆自组网的位置隐私保护技术研究 [J]. 通信学报, 2012, 33(8) : 180 – 189.

[58] Tzeng S-F, Horng S-J, Li T, et al. Enhancing security and privacy for identity-based batch verification scheme in VANETs[J]. IEEE Transactions on Vehicular Technology, 2017, 66(4) : 3235 – 3248.

[59] Yang X, Yi X, Khalil I, et al. A lightweight authentication scheme for vehicular ad hoc networks based on MSR[J]. Vehicular Communications, 2019, 15 : 16 – 27.

[60] Lee C-C, Lai Y-M. Toward a secure batch verification with group testing for VANET[J]. Wireless Networks, 2013, 19(6) : 1441 – 1449.

[61] Akinyele J A, Garman C, Miers I, et al. Charm: a framework for rapidly prototyping cryptosystems[J/OL]. Journal of Cryptographic Engineering, 2013, 3(2) : 111 – 128. http://dx.doi.org/10.1007/s13389-013-0057-3.

哈尔滨工业大学与南方科技大学联合培养研究生

学位论文原创性声明和使用权限

学位论文原创性声明

本人郑重声明：此处所提交的学位论文《基于属性的凭证及其应用》，是本人在导师指导下，在学校攻读学位期间独立进行研究工作所取得的成果，且学位论文中除已标注引用文献的部分外不包含他人完成或已发表的研究成果。对本学位论文的研究工作做出重要贡献的个人和集体，均已在文中以明确方式注明。

作者签名：　　日期：　　年　　月　　日

学位论文使用权限

学位论文是研究生在学校攻读学位期间完成的成果，知识产权归属南方科技大学。学位论文的使用权限如下：

（1）学校可以采用影印、缩印或其他复制手段保存研究生上交的学位论文，并向国家图书馆报送学位论文；（2）学校可以将学位论文部分或全部内容编入有关数据库进行检索和提供相应阅览服务；（3）研究生毕业后发表与此学位论文研究成果相关的学术论文和其他成果时，应征得导师同意，且第一署名单位为南方科技大学。

保密论文在保密期内遵守有关保密规定，解密后适用于此使用权限规定。

本人知悉学位论文的使用权限，并将遵守有关规定。

作者签名：　　日期：　　年　　月　　日

导师签名：　　日期：　　年　　月　　日

致　谢

转眼间研究生生活就快接近尾声了，在这两年中，我学到了不少知识和人生的经验，这得益于周围老师和同学的帮助和启发。

首先我要感谢我的导师王琦老师，从我刚接触密码学开始，到后来的选题，论文的撰写，王老师给予了我不少的指导。王老师不仅在学业上给我带来很多的帮助和启发，也在生活中给予了我很多的鼓励和支持。

还要感谢实验室的学长学弟和学妹们给我的帮助和关怀，你们给我的研究生生活带来了许多的乐趣，给我留下了许多美好的回忆。感谢我的室友及周围的同学，感谢你们平时的关心和帮助。

最后特别感谢我的父母和妹妹对我的支持，让我能够积极乐观地面对生活中的困难与挫折。在未来的日子里，我会继续努力学习，不断超越自己，继续奋斗。