## Abstract

属性基加密作为一个新的密码学原语，被广泛的应用于各种复杂的场景中，因为其拥有在加密的同时还能做到访问控制的特性。但是传统的CP-ABE加密方案存在着一些不足，例如：泄露用户隐私，解密效率低下等。这些不足导致其在实时性要求较高，数据机密性要求较高的场景中（例如：车辆自组网络）难以发挥所长。基于以上的两点，我们提出了A Verifiable Hidden Policy CP-ABE with Decryption Testing Scheme。VHP-CP-ABE拥有如下的特点：隐藏访问策略、外包解密同时能够验证解密结果的正确性。进一步，将其应用到了VANET中。

As a new kind of cryptographic primitive, attribute-based encryption is widely used in various complex scenarios because it has the characteristics of access control while being encrypted. However, the existing CP-ABE encryption scheme has some inherent shortcomings, such as leaking user privacy and inefficient decryption. These shortcomings make it difficult to play a role in scenarios where real-time requirements are high and data confidentiality requirements are high (for example, vehicle ad hoc networks). Based on the above two points, we proposed A Verifiable Hidden Policy CP-ABE with Decryption Testing Scheme. VHPDT-CP-ABE has the following characteristics: hidden access strategy, outsourced decryption can verify the correctness of the decrypted result. Further, it was applied to VANET.

## Introduction

随着云计算和物联网的发展，

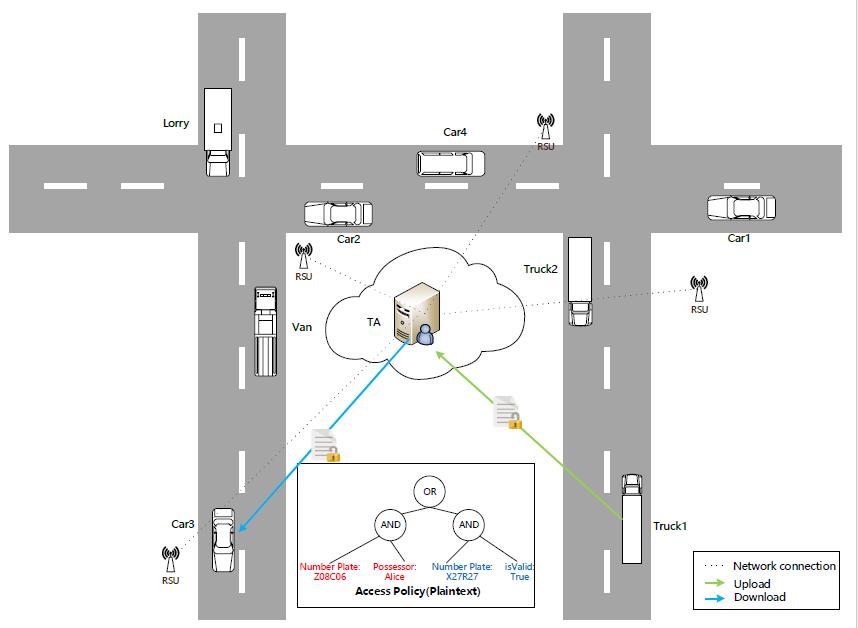


图1是一个典型的VANET的系统架构。为了简便，对于一个VANET，我们可以分为3部分：Vehicle、RSU（Road Side Unit）和CSP。Vehicle是系统中用于信息交换的节点。RSU安置在道路的两旁，为系统的信息交换提供服务。CSP是完全安全的并且值得信任的云服务器。在图1中，我们假设Truck1要通过TA发送消息给Car3。按照标准的CP-ABE或者说按照大部分的CP-ABE方案，将会执行以下的步骤，Truck1首先加密自己发送的信息，然后将加密后的密文和能够解密该密文的访问结构一起发送到CSP，值得注意的是此处的访问结构是以明文的形式存在的，这是由于CP-ABE固有的缺陷造成的。然后CSP在将密文传送给接受者Car3。Car3接收到密文后，用自己的私钥解密密文。以上的步骤是正常的情况，但是我们考虑以下的情形。如果密文在传输过程中被一个攻击者截获，虽然他不能得知加密后的密文的具体信息，但是他可以通过以明文形式传输的访问结构获得一些隐私。在图1中，就可以知道，该条消息是发送给Alice并且她的车牌照是“Z08C06”。很显然这是信息泄露，对于用户来讲这是不可以接受的，因为这可能导致用户被跟踪，诈骗等难以预计的后果。因此，对于访问结构的隐藏就尤为重要。

除此之外，VANET中的节点以嵌入式设备为主，它们虽然方便集成在各种设备之上，但是由于体积的限制，和PC或者服务器相比，运算能力低下，因此如何减少系统的运算开销，也是值得我们关注的地方。

## Our Contribution

在这篇文章中，我们构建了A Verifiable Hidden Policy CP-ABE with Decryption Testing Scheme，它是传统的ABE的扩展，因此能够在加密的同时实现简单、可控、灵活和细粒度的访问控制。我们的方案如果应用到上述的场景中，可以在消息传送路径上完全保护用户的隐私，同时能够高效的进行解密运算，给用户一个良好的使用体验。因此我们的方案是一举多得。

1. VHPDT-CP-ABE采用了树形的访问结构，比起传统的与门形式的访问结构，树形的访问结构能够支持更加灵活的和细粒度的访问控制。
2. 做到的了策略隐藏，在密文的传输过程之中，所有的信息均是被加密的，包括树形的访问策略，因此在传输过程中可以说的完全安全的。
3. 为了减少汽车的本地的解密运算量，将大量的计算外包到VANET中的RSU单元。RSU比起汽车拥有者更强的计算能力。我们在将大量双线性计算外包的同时，也对外包数据进行了部分优化，具体说来就是；有一个Decryption Testing的过程用来减少运算。
4. 进一步，我们的方案能够对外包结果进行验证。以此来避免由于通信网络传输过程中，网络问题造成的错误的外包解密结果。

# Related Work

Sahai和Waters第一次提出提出了模糊身份加密的概念，随后在此基础上CP-ABE被提出。本文主要是针对CP-ABE的策略隐藏和可验证的外包方案以及在VANET中的应用这三个方面进行研究。

为了实现CP-ABE隐私保护的功能。在2008年，Nishide et al. proposed a partially hidden CP-ABE scheme to overcome the above problems. They used AND gate on multi-valued attributes with wild-card access structures and used inner product predicate encryption techniques. Lai et al. improved the Nishide et al. scheme and proposed a fully secure hidden policy scheme with the same access structure used in Nishide et al. The problem with this approach is that the size of the ciphertext grows with the number of attributes and leads to higher computational costs. Li et al. used dual-system cryptography to achieve a completely secure access structure hiding scheme over a composite order group. Hur proposed an attribute-based encryption scheme for hidden policy of the smart grid. Under the premise of hiding the access structure, a scheme for implementing arbitrary monotonic expressions is presented. But the weak points are that the user has a long length of secret key in the scheme, and no security proof is given. Xu et al. proposed a CP-ABE scheme that supports access structure hiding based on the tree access structure, which further improved the expressiveness of the access strategy but efficiency is the bottleneck of the scheme. Yadav et al. gave three states for each attribute in the access structure and calculated its corresponding user secret key and ciphertext to achieve a fully hidden access policy. However, the scheme only supports ”AND” gate, and the expression ability is relatively weak. In 2016, Phuong et al. proposed a new scheme to overcome the ciphertext size problem in hidden strategies. However, the cumbersome user private key calculation process and complex encryption and decryption operations limit its application.

为了解决解密效率低下的问题，Green et al. firstly introduced the notion of ABE with outsourced decryption to solve the issue of low efficiency. Afterwards, Lai et.al optimized Green’s scheme and added verification function to guarantee the correctness of the transformation done by the cloud server. It perfectly settles the issues including low efficiency and correctness of transformation ciphertext, while there are parallel instances in the encryption and decryption algorithms, it can increase communication overhead. Lin et al. used key derivation function(KDF) and random function techniques to successfully reduce excessive communication overhead.

考虑CP-ABE在VANET中的应用。Huang等人是第一个将CP-ABE引入到VANET中的，此后又有一些方案相继被提出。但是如何确保消息以一个高效、灵活并且足够安全的方式分发在VANET中仍然是一个挑战。

## Application in VANET

这一部分，我们将介绍我们方案的在VANET中的实际应用。基于我们的方案，我们构建了一个高效的隐私保护信息分发系统（缩写为：EPPMD system）。图2是我们的EPPMD系统的架构图，从图中可以知道，EPPMD系统由以下几部分组成：

* 汽车集群：汽车集群由参与VANET中的各种各样的汽车组成，它们可以被抽象成VANET中的OSU。是整个系统的消息的参与者与消费者。
* RSU集群：RSU集群由VANET中的RSU单元组成，他们主要为消息的传递以及外包解密服务。
* 云服务器：云服务器由以下几个部分组成，Firewalls、AAS、DB、KGC、KGC、PKS。
* 防火墙用来保证云服务器所在的云环境的安全。
* PKS：私钥生成服务器，用于生成用户的私钥。
* KGC：密钥生成中心，用于生成公钥；
* AAS：属性授权服务器，用于对参与系统的属性进行授权；
* DB：存储已经被授权过的属性的信息。