## 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高速发展，越来越多的人们愿意利用云平台这个媒介进行数据的传递以及分享。同时，越来越多的应用诞生出来满足和便利人们的生活需求。但是，这一切的前提是云计算平台能够提供一个安全、可信的环境在对用户做到细粒度访问控制的同时能够确保用户的隐私不被泄露。

With the rapid development of cloud computing and the Internet of Things, more and more people are willing to use cloud platform as a medium for data transmission and sharing. Meanwhile, innumerable applications are established to satisfy and facilitate life needs of human beings. However, the premise of all this is that the cloud computing platform can provide a secure, trusted environment. Not only can it provide fine-grained access control service for users, it also ensures the privacy of users.

解决以上问题的传统的办法是ABE。因为ABE拥有加密数据，细粒度的访问控制、一对多等特性。具体说来就是，在一个ABE方案中通常拥有3个实体，授权机构、数据拥有者和数据使用者。授权机构生成公钥、主私钥和私钥。数据拥有者使用公钥加密数据并且跟随属性。数据使用者使用私钥解密数据，The data decryption is possible if and only if at least d component

of the attributes in the encrypted data match with attributes in secret key.

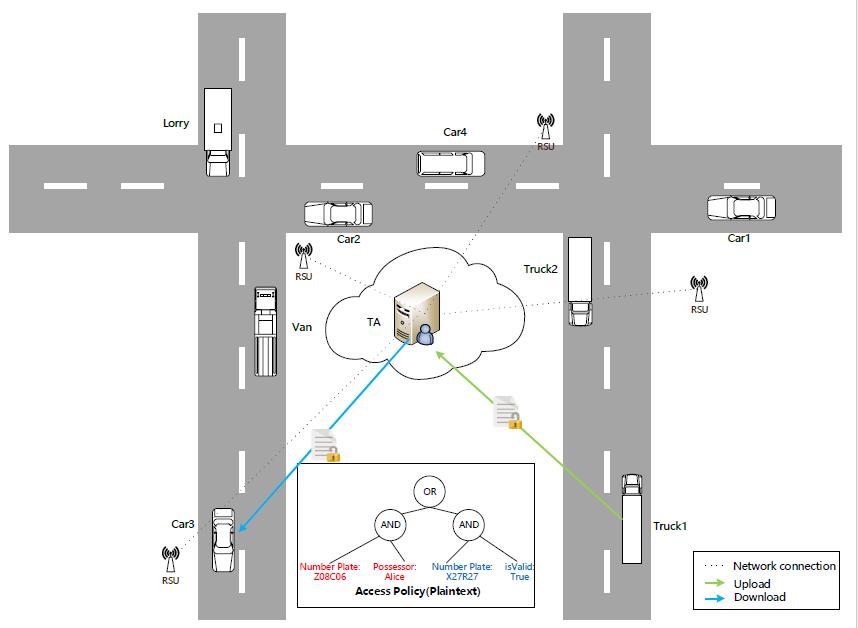
Since attribute-based encryption (ABE) has the characteristics of one-to-many encryption and fine-grained access control, the traditional solution to the above situation is ABE. Specifically, there are usually three entities in an ABE scheme, the data owner, the data consumer and the authority. Authority generates the public key, the master secret key and the private key. Data owner utilizes the public key to encrypt data along with the attributes. Data user can decrypt ciphertext with secret key, and the data decryption is possible if and only if at least d component of the attributes in the encrypted data match with attributes in private key. Here let us take the VANET system as an example.

尽管ABE方案看上去可行，但是仍有一些细致和深入的问题需要我们考虑。这里我们拿VANET做例子。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：OBU、RSU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，隐私保护在信息传递中十分重要。

Despite the ABE scheme seems feasible, there are still some meticulous and in-depth questions we need to consider. Figure 1 shows a typical VANET system architecture. For a VANET system, it can be divided into three parts: OBU (On-Board Unit), RSU (Road Side Unit) and CSP (Cloud Server Provider). OBU is abstracted from vehicle sensor and serves as information transmission node in the system. The RSU is set on both sides of the road to provide services for information transmission in system and CSP is a completely secure and trustworthy cloud server. In Figure1, we assume that Truck1 will send a message to Car3 via CSP. Refer to standard or most ABE schemes, the following steps will be executed. Truck1 first encrypts the data to generate ciphertext that will be sent to CSP along with the access structure. Due to the inherent defects of ABE, it is worth nothing that the access structure here exists in plaintext. The CSP then transmits the ciphertext to the recipient Car3. After receiving the ciphertext, Car3 decrypts the ciphertext with its own private key. The above steps are normal, but we consider the following situation. If the ciphertext is intercepted by a malicious attacker during transmission, although the malicious attacker cannot read the specific information of the ciphertext, he can obtain some sensitive information through the access structure transmitted in plaintext format. For example, in Figure1, the malicious attacker may get the information that is sent to Alice and her license plate is Z08C06. This is information disclosure obviously. It is unacceptable to users because it can lead to unpredictable consequences such as tracking, telecom fraud and so on.

进一步，目前存在的大多数的ABE方案大多采用椭圆曲线构造生成，在解密过程中包含了大量的耗时的配对运算，并且解密耗时会随着属性的个数递增。在VANET中，OBU和RSU大部分是嵌入式设备，又有着较小的体积，同时也有着较差的性能。在运算方面往往不如普通的PC。上文提到，VANET是实时性要求较高的系统，因此效率是VANET中又一个决定性的因素。

Further, most of the existing ABE schemes are generated by elliptic curves. A lot of time-consuming pairing operations are involved in the decryption algorithm, and the decryption time increases with the number of attributes. In VANET system, OBU and RSU are mostly resource-limited embedded devices with tiny size, which have poor performance compared to desktops in term of computing. In addition, VANET system is a high real-time system, hence, efficiency is the other decisive factor for VANET system.



## 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。

If our solution is applied to the above scenario, the user's privacy can be completely protected on the message transmission path, and the decryption operation can be performed efficiently, giving the user a good experience. Therefore, our plan is to win in one fell swoop. Multi-faceted

1. VHPDT introducs a tree-based access structure which supports more flexible and fine-grained access control than AND gate access structure.
2. All information is encrypted, during the ciphertext transmission process, including the hidden policy which exists in plaintext in mostly ABE schemes. Therefore, it is fully secure during the transmission process.
3. In order to reduce the amount of decryption operations of the OBU, we outsource some time-consuming operations to RSU in the VANET system, because RSU is more computation capable than OBU. Further, to improve the efficient of outsourcing, we partially optimize the outsourcing algorithm, concretely, we add a Decryption Testing algorithm which is used to reduce redundant operations. After Decryption Testing algorithm, OBU can verify the correctness of the results.

# 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：EPPMT system）。图2是我们的EPPMT系统的架构图，从图中可以知道，EPPMT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、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。

防火墙用于隔绝云环境与外部网络环境，为其他服务器提供一个安全域的保障。

In this section, we introduce the practical application of our scheme in VANET. Based on above idea, we construct an efficient privacy-preserving message transmission system named EPPMT system. Fig. 2 illustrates the architecture of EPPMT system and it consists of the following components:

# Performance Analysis

## Functionality Comparison

## Theoretical Analysis

考虑到不同的访问结构对方案的影响，因此为了公平起见，我们在理论分析和实验分析部分我们只考虑树形结构的方案。在表二中，我们的方案和已有的方案在公钥、私钥和密文的长度这三方面进行了对比。在私钥方面，所有的方案的私钥的长度都是线性增长的，只不过不同的方案的增长率不同，我们的方案的增长率最低为k，其他方案的增长率分别为3k，3k，2n。在公钥长度方面，我们的方案比Hur和Helil的方案增长率较高，但是和Muller的方案拥有着相同的增长率——N+4。在密文长度方面，由于我们引入和末端内部节点的概念，因此密文长度和末端结点的数量还有系统中的属性数量相关，当末端结点数量较少时，密文长度也更少。

在表四中，我们比较了不同方案的效率，包括加密和解密效率两个主要的方面。在加密层面，由于我们的方案引入了末端内部结点，因此我们的方案的加密效率和末端内部节点的数量以及系统的属性数有关。在解密方面，我们的方案和Hur以及Helil的方案都是常数量级，但是由于我们的方案不包括配对运算，因此更加高效。

## Experimental Simulation

为了验证上述理论分析的正确性，我们仿真了我们的方案并且实现了上述文章中的方案。所有的实验均是基于Java Pairing-Based Library (JPBC). 为了达到安全性，所有的实验使用160位的椭圆曲线组，它是由在512位有限域上的超奇异曲线生成的。 最后，所有的实验运行在一台小米6智能手机中，它的配置是1.9GHz的骁龙835和3GB Random Access Memory并且运行了MIUI 10.2 操作系统（基于安卓9.0）。

实验结果如图4所示。图4的a和b分别展示了加密时间和解密时间随着属性数量变化关系。从图4a中我们可以知道，4个方案的加密时间都是随着属性的变化近乎成线性变化的。当属性的数量较少时，例如为2，这时候4个方案的加密时间近乎相同，分别为：500ms，500ms，500ms，500ms。当属性数量从2增长到20时，因为增长率的不同，4个方案的加密时间出现了明显的变化，Muller的方案耗时最多，大约是4500ms，我们的方案、Helil和Hur次之，为3400ms，2700ms，2500ms。从图7b中，我们可以知道，只有Muller的方案的解密时间随着属性的增加而增加，当属性是2的时候，解密时间大约是800ms，属性增长到20的时候，解密时间增长到5500ms。Hur、Helil的方案和我们的方案的解密时间是一条水平的直线。其中Hur和Helil的方案的解密时间大致相同，为250ms。我们的方案的解密时间最少，为90ms。

此外，我们还比较了几个方案的私钥的存储开销，如图5所示。Muller的方案拥有最高的存储开销在4个方案中。它从2.8KB增长到7.8KB，当属性数量从10增长到30。Hur和Helil的方案总是有着相似的开销，当属性数量为10，20，30，存储开销为2.2KB，4.7KB，6.8KB。不论属性的数量如何改变，我们的方案总是拥有着最小的私钥开销。相似的，当属性数量被设置为10，20，30时，我们的方案的私钥的开销大概为1KB，1.75KB，2.37KB。和消耗最高的Muller方案对比，仅仅需要花费30%左右的空间。