## 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 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 traditional CP-ABE encryption scheme has some 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. VHP-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.