AW-UBI: 基于车辆数据作为可认证证据的 UBI 方案

颜　俊　岳笑含
沈阳工业大学　辽宁沈阳　110870

摘　要：在车辆保险行业，基于使用的保险 (Usage-Based Insurance, UBI) 变为越来越受欢迎。UBI 车辆保险区别于传统的保险方案，其保费收取与驾驶行为所表现出的驾驶风格密切相关。然而，到目前为止，关于商用车 UBI 产品的隐私保护方案报道却少之又少，并且现有的 UBI 车辆保险方案普遍存在车辆数据隐私、保费计算的可验证性、保费计算数据的可认证性及交易的公开可验证性的问题。本文针对目前存在的问题，提出了一个面向 UBI 基于具有可认证性零知识证明的隐私保护方案。

关键词：车辆保险；　基于使用的保险 (UBI)；　ZK-SNARK；　可认证数据

AW-UBI: A Vehicle Data as Authenticated Witness of UBI

Jun Yan, Xiaohan Yue
Shenyang University of Technology,Shenyang,Liaoning,110870

Abstract: In the vehicle insurance industry, Usage-Based Insurance (UBI) has become increasingly popular. UBI vehicle insurance differs from traditional insurance schemes in that the premium charged is closely related to the driving style exhibited by the driver. However, so far there have been few reports on privacy protection schemes for commercial vehicle UBI products, and existing UBI vehicle insurance schemes generally suffer from problems such as vehicle data privacy, verifiability of premium calculation, verifiability of premium calculation data, and public verifiability of transactions. In this paper, we propose a privacy protection scheme for UBI based on zero-knowledge proofs with verifiability for UBI data.

Keywords: vehicle insurance; usage-based insurance (UBI); ZK-SNARK; Verifiable data

引言

长期以来，车辆已经深刻影响了人民生活和工作的方式，成为每个家庭必不可少的成员之一。为了保障驾驶员的行车安全和个人利益，车辆保险已经成为每位驾驶员出行保障的不二选择，同时也成为了每名驾驶员的固定支出。传统的车辆保险费每年根据参保用户的静态数据进行保费计算，如参保车辆驾驶员的年龄、参保车辆的种类、交通违章情况和保险周期内的事故情况。这样计算保费的方式无法激励参保用户更安全地驾驶，因为车辆的保险费不是根据一辆汽车的具体行驶情况计算的。与前者相比，基于使用的 UBI 车辆保险可以根据驾驶情况和驾驶模式计算保险费，例如里程 [1]、驾驶时间、车速 [2]、加速度等综合因素 [3]。如果有详细的驾驶情况和驾驶模式数据 [2]，UBI 车辆保险可以动态且更准确地向参保用户进行收费。

但出于隐私方面的考虑，很多司机不愿意将车辆数据发送给保险公司 (或第三方)。并且保险公司为防止参保用户进行保险诈骗，一般 UBI 车辆保险都会要求参保用户提供详细的车辆数据，其中包括车辆行程的时间、车辆位置和距离，以及车辆速度和加速度等资料。这些车辆数据通常由保险公司或第三方存储，一旦这些数据泄露给对手，对手就可以轻易地查到例如：参保用户去过的时间和地点，以及其的驾驶模式和习惯。

因此车辆数据的隐私保护问题直接影响了 UBI 车辆保险的实用性。其中如何在 UBI 策略中在能够确保车辆数据隐私的前提下，保障保费计算的可验证性、保费计算数据的可认证性及交易的公开可验证性变得尤为重要。因此如何高效的解决上述问题成为了人们最关心的问题。

一、本文的主要贡献

综上所述，本文针对上文所提出的 UBI 车辆保险的隐私保护方案的普遍缺陷进行完善，并给出解决方案及性能测试及分析，以下是本文的主要贡献如下：

基于功能性和安全性需求，我们提出了 AW-UBI 方案，并且我们给出了 AW-UBI 方案的框架，并且定义了 AW-UBI 方案中参与的实体及相关算法；然后基于 AW-UBI 方案框架，我们进一步给出了 AW-UBI 方案的构建。

在通用可组合性框架下，针对 UBI 车辆保险中普

遍存在的车辆数据隐私、保费计算的可验证性、保费计算数据的可认证性及交易的公开可验证性问题。我们应用零知识证明技术、可验证计算技术、聚合签名技术及区块链技术对上述问题进行了结合，然后给出了更契合AW-UBI方案的安全定义。

针对AW-UBI方案中的安全定义，基于ADSNARK方案对数据可验证性扩展。目的是防止参保用户使用非法数据计算保费，进行骗保，保证通信的正常进行。

二、系统模型和安全需求

2.1 系统模型

本文定义的参与实体如下，系统模型如图1所示。

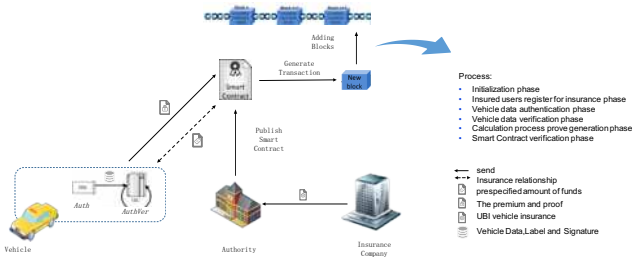

图1 系统模型

权威机构(Insurance Regulatory Authority)：选取安全参数，接受保险公司发送的UBI车辆保险方案并且发布智能合约。

保险公司(Insurance Company)：拟定UBI车辆保险并将拟定好的UBI车辆保险交由给权威机构审核。智能合约的收款方，为参保人提供UBI车辆保险服务。

车载传感器(OBD)：安装在车辆上的车辆自诊断系统。用于周期性收集车辆行驶中的数据，数据包括但不限于速度、加速、里程等类型。

车辆主控(OBC)：和OBD相连接，接受OBD发送的签名值和对应数据与标签，标签可以标识数据的产生时间与数据类型，并对签名值进行验证，以确保数据是由OBD发送的。

智能合约(Smart Contract)：由权威机构设计并且发布，智能合约包含两个算法，一个为参保人加入智能合约的注册算法。另一个为保费验证算法。

2.2 安全需求

为了实现我们的目的，本文的方案需要满足以下的一些安全和隐私需求：

数据隐私性：敌手除了能够从通信信道中窃取到车辆发送的保费与证明保费的证明以外，不能再获取到任何泄露车辆数据的信息。

数据是真实的情况下的保费计算可验证性：车辆保费由OBC在车辆本地使用OBD提供的真实数据进行计算得出，智能合约在接受到保费与证明保费的证明之后，在不知道车辆数据的前提下，能够验证保费确实是通过OBD提供的真实数据进行计算得出。

透明性：在智能合约上进行保费验证过程和保险续约的交易过程是公开的。并且将交易过程会被写入区块链，以实现交易的公开和不可篡改。

三、方案设计

在本节中，提出了一种基于车辆数据作为可认证证据的UBI方案，并给出了方案的设计。我们假设方案中实体的交互是通过安全信道完成的。

1）初始化阶段：公共参数的生成与密钥和证明使用参数的初始化。具体步骤如下：

1.1）初始化算法：权威机构使用安全参数生成公共参数。其中安全参数包括一组双线性群与群中的生成元，和一个非对称双线性映射。

1.2）密钥生成算法:OBD生产方根据权威机构的公共参数生成密钥其中为私钥，为验证密钥，OBD生产方会使用权威机构的公共参数与密钥生成的公共参数组成公用认证参数 。

1.3）证明用参数生成算法：权威机构通过分析从保险公司设计的UBI车辆保险方案，首先权威机构设置随机化参数，然后权威机构通过电路实例算法实现保险公司设计的UBI车辆保险方案的实例化，根据实例算法的初始化计算生成必要参数。

2）参保用户加入UBI车辆保险阶段：参保用户参加智能合约UBI车辆保险方案，参保用户将在智能合约上注册，并向智能合约中存入预先规定的资金作为预付款承诺。

3）车辆对收集的行驶数据进行签名阶段。行驶数据签名算法:OBD收集车辆行驶的信息，并将这些信息用标签 去标识数据的产生时间和数据类型如里程、速度、加速度等。并对数据信息与数据标签使用进行签名，生成签名值。并将签名值、车辆行驶数据标签和车辆行驶数据传给OBC。

4）车辆对收集的行驶数据进行验证。行驶数据验证算法:OBC在收到OBD发送的签名值、车辆行驶数据标签和车辆行驶数据时，对这些数据通过进行验证当验证成立输出1，否则为0。以确保行驶数据是由OBD发送的。

5）车辆保费生成与车辆保费生成的证明生成。证明算法:OBC会使用权威机构提供的公共参数和从OBD接受到的数据与签名值，进行计算UBI车辆保险的保费和保费证明。

6）智能合约验证保费和证明。保费验证算法：验证证明阶段，当UBI智能合约接受到OBC发送的保费与证明后，智能合约对将对保费与证明进行验证。验证不通过时：输出0，通过时输出1。验证通过后对该用户的预付账户进行正确扣费，将金额打入保险公司账户，将交易账单上传到区块链上。

四、结束语

本文提出并解决了UBI车辆保险方案中保护隐私数据的问题，重点讨论了车辆行驶数据需要被认证以确定

保费结果正确性的情况，重点讨论了保费的生成是通过被认证车辆数据生成的，并且保费的计算是通过所要求的保险方案计算得出的，通过验证算法即能保证车辆数据的认证性，并且不需要披露原始车辆行驶数据。AW-UBI 也继承了现有 SNARK 的一些局限性，例如，不同的保险公司会设计不同的保险方案，而不同的 UBI 保险方案意味着不同的逻辑电路，但逻辑复杂的电路会导致约束数量的增加，进而影响证明生成的效率。最近 [11] 基于配对友好型的曲线有效的提升了 SNARK(例如 :Groth16) 的配对运算效率，这样或许能提高基于 SNARK 证明的保险方案的证明生成效率，本文把研究更方便、更高效的 UBI 保险计算模型作为今后的工作。

参考文献：

[1] Dijksterhuis, C.; Lewis-Evans, B.; Jelijs, B.; de Waard, D.; Brookhuis, K.; Tucha, O. The impact of immediate or delayed feedback on driving behaviour in a simulated Pay-As-You-Drive system. Accid. Anal. Prev. 2015, 75, 93 - 104.

[2] Agerholm, N.; Waagepetersen, R.; Tradisauskas, N.; Harms, L.; Lahrmann, H. Preliminary results from the Danish Intelligent Speed Adaptation Project Pay As You Speed. IET Intell. T ransp. Syst. 2008, 2, 143 - 153.

[3] Nai, W.; Zhang, F.; Dong, D.; Chen, Y .; Yu, Y .; Zheng, W. Fuzzy Risk Mode and Effect Analysis Based on Raw Driving Data for Pay-How-You-Drive V ehicle Insurance. In Proceedings of the IEEE International Conference on Big Data Analysis (ICBDA), Hangzhou, China, 12 - 14 March 2016..