# 基于国密SM9的分层标识签名方案

谢 佳[1*],栾小杰[1],范长友[1],王鲁玉[1],高军涛[2],王保仓[2]

(1. 河南财经政法大学计算机与信息工程学院,河南郑州 450046;2. 西安电子科技大学通信工程学院,陕西西安 710071)

**摘 要:** 我国自主研发的SM9密码算法是重要的商用密码标准和国家标准,对于密码算法的国产化替代具有关键作用。然而,原始SM9数字签名作为标识签名机制,存在不具备分层特征的局限性,在大规模网络环境中极易因用户量激增导致密钥生成中心压力过大和网络拥堵。为解决这一难题,本文首次提出了一种基于国密SM9算法的分层标识签名方案。方案创造性地引入分层签名技术,通过各级节点共同分担密钥生成任务,有效减轻了密钥生成中心的私钥生成与分发压力,完美适用于车联网、区块链等大规模、多层级网络场景。在技术实现上,为了适配SM9算法,本方案基于素数阶群,采用高效的分层技术,完成由上一层签名私钥到下一层级签名私钥的分配,以此来形成一种层级式的私钥更新机制;紧接着用户再根据其签名私钥来进行数字签名,生成的签名值仅由三个群元素构成,相较于原始SM9算法仅增加一个群元素,并实现了常数级签名长度,与层级深度无关。在随机谕言机模型下,给出了方案的严格安全性证明,证明方案满足选择消息和身份攻击下的存在性不可伪造,且方案的安全性可规约至$(q,n)$-SDH困难问题。理论分析与实验结果表明,本方案在签名生成和验证效率上具有显著优势:随着系统层数$k$的增加,本方案的签名生成和签名验证时间趋于常量级别,明显优于现有基于双线性对的分层标识签名方案。特别地,当系统层数$k$为2~10时,签名生成和验证时间分别约为2.24 ms和36.08 ms,签名和验证效率较现有最优的分层签名方案分别提升0.03~2.79倍和0.87~1.27倍。且随着$k$的增大,效率提升就越大,当$k$为100时,签名生成和验证效率较现有最优的分层签名方案分别提升约34倍和4.5倍。最后,将本方案应用于车联网身份认证场景,成功解决了车联网环境中因用户量激增而导致的网络拥堵问题,实现了轻量化与去中心化的身份认证机制,为构建高效、安全的国产化大规模网络环境提供了重要的技术支撑。

**关键词:** 分层签名;SM9;标识签名;车联网身份认证;定长签名

**基金项目:** 国家自然科学基金(No.61802110);河南省重点研发与推广专项(科技攻关)项目(No.242102210149,No.222102210326);河南省高等学校重点科研项目(No.23A413001,No.25A413008);河南财经政法大学黄廷方/信和青年学者资助计划;河南财经政法大学校级研究课题

**中图分类号:** TP309 **文献标识码:** A **文章编号:** 0372-2112(2026)02-0710-13

**电子学报URL:**http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20250954

# Hierarchical Identity-Based Signature Scheme Based on SM9

XIE Jia[1*], LUAN Xiaojie[1], FAN Changyou[1], WANG Luyu[1], GAO Juntao[2], WANG Baocang[2]

(1. *School of Computer and Information Engineering*, *Henan University of Economics and Law*, *Zhengzhou*, *Henan* 450046, *China*;
2. *School of Telecommunications Engineering*, *Xidian University*, *Xi'an*, *Shaanxi* 710071, *China*)

**Abstract:** The SM9 cryptographic algorithm, independently developed by China, serves as a critical commercial cryptography standard and national standard, playing a key role in the localization and substitution of cryptographic algorithms. However, the original SM9 digital signature, as an identity-based signature mechanism, suffers from the limitation of not supporting hierarchical features. In large-scale network environments, this can easily lead to excessive pressure on the key generation center and network congestion due to the surge in the number of users. To address this challenge, this paper proposes the first hierarchical identity-based signature scheme based on the national cryptographic SM9 algorithm. The scheme innovatively introduces hierarchical signature technology, distributing the key generation task across multiple levels of nodes, effectively alleviating the private key generation and distribution pressure on the key generation center. It is ideally suited for large-scale, multi-layered network scenarios such as the Internet of Vehicles and blockchain. In terms of technical implementation, to adapt to the SM9 algorithm, this scheme is based on prime-order groups and employs efficient hierarchical technology to allocate signature private keys from the upper level to the next level, thereby forming a hierarchical private key update mechanism. Subsequently, users generate digital signatures based on their signature private keys. The resulting signature value consists of only three group elements, adding just one more group element compared to the original

收稿日期:2025-12-19;录用日期:2026-02-03;责任编委:李雄

*通信作者:谢佳

SM9 algorithm, and achieves a constant signature length independent of the hierarchical depth. Under the random oracle model, a rigorous security proof of the scheme is provided, demonstrating that the scheme satisfies existential unforgeability under chosen message and identity attacks, and its security can be reduced to the $(q,n)$-SDH hardness problem. Theoretical analysis and experimental results show that the proposed scheme has significant advantages in signature generation and verification efficiency. As the number of system layers $k$ increases, the signature generation and verification time of this scheme tends to remain constant, significantly outperforming existing hierarchical identity-based signature schemes based on bilinear pairings. Specifically, when the number of system layers $k$ ranges from 2 to 10, the signature generation and verification times are approximately 2.24 ms and 36.08 ms, respectively, improving efficiency by 0.03 to 2.79 times and 0.87 to 1.27 times compared to the current optimal hierarchical signature schemes. Moreover, as $k$ increases, the efficiency improvement becomes more pronounced: when $k$ is 100, the signature generation and verification efficiency are enhanced by approximately 34 times and 4.5 times, respectively, compared to the existing optimal hierarchical signature schemes. Finally, the proposed scheme is applied to the identity authentication scenario of the Internet of Vehicles, successfully resolving network congestion caused by the surge in users in the IoV environment. It realizes a lightweight and decentralized identity authentication mechanism, providing crucial technical support for building efficient and secure large-scale network environments with localized cryptographic solutions.

Keywords: hierarchical identity-based signature; SM9; identity-based signature; internet of vehicles identity authentication; fixed length signature

Foundation Item(s): National Natural Science Foundation of China (No.61802110); Key Research and Development and Promotion Program of Henan Province (No.242102210149, No.222102210326); Key Research Foundation for Higher Education of Henan Province (No.23A413001, No.25A413008); the NG Teng Fong/Sino Foundation for Youth in Henan Universityof Economics and Law, and the Research Foundation in Henan University of Economics and Law

## 0　引言

在传统公钥基础设施(Public Key Infrastructure, PKI)中,用户身份与公钥的绑定是通过数字证书实现的,但其证书签发、存储与验证流程复杂,存在管理效率低下的问题。为此,Shamir[1]于1984年在美密会议上首次提出了基于身份的密码思想,开创了标识密码体制(Identity-Based Cryptography, IBC)的研究方向。在此体系中,用户公钥是基于其唯一身份标识(如身份证号、邮箱等)派生而来,省去了数字证书管理的开销。然而,IBC体系中用户私钥不再由用户自己生成,而是由私钥生成中心(Private Key Generator, PKG)统一生成。PKG认证用户标识后,基于系统公共参数和主私钥生成并分发用户私钥。此后,用户才可凭借该私钥完成对消息或数据的签名。

自标识密码的概念提出后,迅速吸引了学术界及工业界的密切关注。2001年,Boneh等人[2]在美密会议上提出了首个安全且实用的标识加密(Identity-Based Encryption, IBE)方案,其安全性在随机预言机模型下得到了证明,该方案标志着标识密码体制由理论阶段进入了可应用阶段,为推动IBE体制的深入研究与实际应用奠定了研究基础。然而,该架构中所有用户的私钥均需由PKG统一生成并分发。随着系统规模的扩展和用户量的激增,PKG在身份验证、私钥计算及安全传输等方面的负荷急剧增加,容易引发网络拥堵,难以适应高并发和实时性服务需求。这种集中式的密钥管理模式严重限制了标识密码技术在大规模网络环境中的推广与应用,成为亟需解决的关键问题。

为了解决大规模网络环境中单一PKG工作繁重的问题,2002年,Horwitz等人[3]在欧密会议上提出了分层标识加密(Hierarchical Identity-Based Encryption, HIBE)的概念,为多层次身份管理提供了新的解决思路。在HIBE系统中,通过根PKG将私钥生成与身份认证任务委派给下级PKG,形成分层管理结构。该系统具有局部安全性的特点,即某一层私钥泄露仅影响后续层级,而不危及前续层级密钥安全。同年,Gentry等人[4]在亚密会议上提出了首个有效的HIBE方案,奠定了分层标识密码(Hierarchical Identity-Based Cryptography, HIBC)体制研究的基础。随后多项研究致力于优化方案效率与安全性:2004年,Boneh等人[5]在欧密会议上提出了标准模型下满足判定性双线性迪菲-赫尔曼(Desidional Bilinear Diffie-Hellman, DBDH)假设的HIBE方案,但方案的密文长度随着层数的增加而线性增加。同年,Chow等人[6]提出了首个可证明安全的分层标识签名(Hierarchical Identity-Based Signature, HIBS)方案,在随机预言机模型下,该方案的安全性可归约到计算性迪菲-赫尔曼(Computational Diffie-Hellman, CDH)假设,但方案的签名长度随着层数的增加而线性增加。2005年,Boneh等人[7]和Yuen等人[8]分别提出了具有固定密文长度的HIBE方案和具有固定签名长度的HIBS方案。2006年,Au等

人[9]提出不依赖随机预言机且固定密文长度和固定签名长度的HIBE和HIBS方案。2011年，吴青等人[10]在标准模型中提出了基于CDH假设且固定签名长度的HIBS方案。

为了实现密码算法的自主可控和国产化替代，我国于2006年自主研制SM9标识密码体系[11]，提供了包括数字签名、公钥加密等在内的多种密码原语。其中，其数字签名算法于2016年正式成为国家商用密码标准，2020年晋升为国家标准，更于2021年成为ISO/IEC国际标准，标志着其技术成熟度和国际认可度。然而，SM9算法本身并不支持分层结构，在实际大规模应用中，在用户数量激增时面临巨大的计算与通信压力，容易引发网络拥堵，从而严重制约系统整体效率。尽管国内学者对SM9算法开展了广泛且深入的研究，并取得了许多优秀的成果，涌现出包括环签名[12-17]、聚合签名[18]以及一些具有特殊属性的签名[19-24]；同时还包括对SM9算法的安全性证明[25-26]和在区块链技术中的应用[14,27]等在内的一系列成果，但是在分层签名领域仍存在明显空白，截至目前并未在国际主流期刊和会议上发现针对SM9分层标识签名方案的任何相关研究成果，仅有个别文献探讨了基于SM9的分层加密方案[28-30]。因此，构建支持分层架构的SM9签名方案，对提升系统可扩展性和实现更高效率的密钥管理具有重要的理论与实际意义。

故本文在以上基础上作出以下主要贡献：

（1）将国密SM9与分层签名技术相结合，提出了首个基于SM9常数级别大小的分层签名方案，并将其应用到车联网的身份认证场景中，在实现国产化替代的同时，也解决了当前车联网环境中认证效率较低的问题。

（2）在随机谕言机模型下，给出了方案的安全性证明，方案满足选择消息和身份攻击下的存在性不可伪造。方案的安全性可规约至$(q,n)$-SDH困难问题。

（3）通过理论分析与实验对比表明，本文方案在签名生成和签名验证上存在明显的性能优势：当系统层数$k$为2~10时，签名生成与验证时间分别约为2.24 ms和36.08 ms，签名和验证效率较现有最优的分层签名方案分别提升0.03~2.79倍和0.87~1.27倍。

## 1 预备知识

### 1.1 符号说明

表1是对本文使用符号的解释说明。

### 1.2 双线性群

令$\mathbb{G}_1,\mathbb{G}_2$是$N$阶加法循环群，$\mathbb{G}_T$是$N$阶乘法循环群，$P,Q$分别为群$\mathbb{G}_1,\mathbb{G}_2$的生成元，其双线性映射$e$：$\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$满足：

（1）双线性：$\forall a,b\in\mathbb{Z}_N^*$和$P\in\mathbb{G}_1,Q\in\mathbb{G}_2$，有$e(aP,bQ)=e(P,Q)^{ab}$。

（2）非退化性：$\exists P\in\mathbb{G}_1,Q\in\mathbb{G}_2$，使得$e(P,Q)\neq 1_{\mathbb{G}_T}$。

（3）可计算性：$\forall P\in\mathbb{G}_1,Q\in\mathbb{G}_2$，$e(P,Q)$可以被计算。

**表1 符号说明**

Table 1 Symbol description

| 符号 | 含义 |
|---|---|
| $\lambda$ | 安全参数 |
| $n$ | 系统最大层数 |
| $k$ | 系统当前层数 |
| $N,p$ | 大素数 |
| $\mathbb{Z}_N^*$ | 整数集合$\{1,2,\cdots,N\}$ |
| $F_p$ | 阶为素数$p$的有限域 |
| $d_1^*,d_2^*$ | 第1层用户私钥 |
| $d_1',d_2',d_k'd_{k+1}',\cdots,d_n'$ | 第$k-1$层用户私钥 |
| $d_1,d_2,d_{k+1}d_{k+2},\cdots,d_n$ | 第$k$层用户私钥 |

### 1.3 困难问题假设

**定义1** $q$-SDH问题。已知$q+2$个元素$(P,Q,aQ,a^2Q,\cdots,a^qQ)\in\mathbb{G}_1\times\mathbb{G}_2^{q+1}$，$q$-SDH问题即为找到一个二元组$\left(c,\frac{1}{c+a}P\right)$，其中$a$未知，$c\in\mathbb{Z}_N^*$。

在$c\in\mathbb{Z}_N^*$，$a$未知的情况下，且要在有限时间内构造$\frac{1}{c+a}P$，成功的概率几乎为0，故$q$-SDH问题是困难的。

**定义2** $(q,n)$-SDH问题[26,28]。已知双线性群$\mathrm{bp}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,N)$，元素集合$(c,P,bP,aP,a^2P,\cdots,a^qP,\frac{1}{(a+c)^2}P,\frac{1}{(a+c)^3}P,\cdots,\frac{1}{(a+c)^n}P,Q,bQ,aQ,a^2Q,\cdots,a^{n+1}Q)$，$(q,n)$-SDH问题即找到一个二元组$\left(c,\frac{1}{c+a}P\right)$，其中$c\in\mathbb{Z}_N^*$，且$a$未知。

### 1.4 SM9数字签名算法

SM9数字签名算法主要分为4个阶段，分别是参数生成、私钥提取、签名生成和签名验证。

（1）参数生成。以安全参数$\lambda$为输入，构建双线性对$e$：$\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$，其中$\mathbb{G}_1$和$\mathbb{G}_2$分别是阶为$N$的加法群，$\mathbb{G}_T$为阶为$N$的乘法群，$P_1$和$P_2$分别是$\mathbb{G}_1$和$\mathbb{G}_2$的生成元，再选取两个密码杂凑函数$H_1$、$H_2$：$\{0,1\}\to\mathbb{Z}_N^*$，KGC选取$\alpha\in\mathbb{Z}_N^*$作为主私钥msk，计算$P_{\mathrm{pub}}=\alpha P_2$，并计算$g=e(P_1,P_{\mathrm{pub}})$。最后，输出系统主公钥$\mathrm{mpk}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,N,P_1,P_2,P_{\mathrm{pub}},g,H_1,H_2)$作为下面阶段的默认输入。

(2)私钥提取。输入用户的身份标识ID,计算有限域上的非零元素 $t_1=H_1(\mathrm{ID})+\alpha$,然后计算 $\mathrm{sk}_{\mathrm{ID}}=\alpha\cdot t_1^{-1}\cdot P_1$,并输出用户的私钥 $\mathrm{sk}_{\mathrm{ID}}$。

(3)签名生成。输入用户的身份标识ID,签名私钥 $\mathrm{sk}_{\mathrm{ID}}$ 和消息 $M$,选取随机数 $r\in\mathbb{Z}_N^*$,分别计算 $h=H_2(M\|g^r,N)$,$S=(r-h)\mathrm{sk}_{\mathrm{ID}}$,并输出签名 $\sigma=(h,S)$。

(4)签名验证。输入用户的标识ID,消息 $M$ 和签名 $\sigma$,计算 $P=H_1(\mathrm{ID})\cdot P_2+P_{\mathrm{pub}}$,验证 $e(S,P)g^h=g^r$ 是否成立。若成立则验证成功,否则验证失败。

## 2　分层标识签名

### 2.1　形式化定义

分层标识签名是一种多层次的数字签名方案,允许签名者将签名权限分层委托给下层用户。分层标识签名方案主要包含以下4个算法(Setup, KeyGen, Sign, Verify):

(1)$(\mathrm{mpk},\mathrm{msk})\leftarrow\mathrm{Setup}(\lambda,n)$,参数生成算法。输入安全参数 $\lambda$ 和系统最大深度 $n$,输出系统主密钥对(mpk, msk),系统公开mpk,KGC秘密保存msk。

(2)$\mathrm{sk}_{\mathrm{ID}|_k}\leftarrow\mathrm{KeyGen}(\mathrm{mpk},\mathrm{sk}_{\mathrm{ID}|_{k-1}},\mathrm{ID}|_k)$,私钥提取算法。输入mpk、第 $k-1$ 层用户的私钥 $\mathrm{sk}_{\mathrm{ID}|_{k-1}}$ 和第 $k$ 层用户的标识 $\mathrm{ID}|_k$,输出第 $k$ 层用户的私钥 $\mathrm{sk}_{\mathrm{ID}|_k}$,其中 $\mathrm{ID}|_k=(\mathrm{ID}|_{k-1},\mathrm{ID}_k)$,$1<k\leqslant n$。

(3)$\sigma\leftarrow\mathrm{Sign}(\mathrm{mpk},M,\mathrm{sk}_{\mathrm{ID}|_k})$,签名生成算法。输入系统主公钥mpk、待签名消息 $M$ 和第 $k$ 层用户的私钥 $\mathrm{sk}_{\mathrm{ID}|_k}$,输出签名值 $\sigma$。

(4) $\mathrm{accept/reject}\leftarrow\mathrm{Verify}(\mathrm{mpk},\mathrm{ID}|_k,M',\sigma')$,签名验证算法。输入系统主公钥mpk、签名者的标识 $\mathrm{ID}|_k=(\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_k)$,以及被签名的消息 $M'$ 和待验证的签名值 $\sigma'$,若验证成功,输出accept;验证失败,输出reject。

对于分层标识签名方案的正确性表现为:对于合法的签名,验证总是成功的;对于不合法的验证总是失败的。即

$$\Pr\left[\mathrm{Verify}(\mathrm{mpk},\mathrm{ID}|_k,M',\sigma')\right.$$

$$\left.=\mathrm{accept}\left|\begin{array}{l}(\mathrm{mpk},\mathrm{msk})\leftarrow\mathrm{Setup}(\lambda,n)\\ \mathrm{sk}_{\mathrm{ID}|_k}\leftarrow\mathrm{KeyGen}(\mathrm{mpk},\mathrm{sk}_{\mathrm{ID}|_{k-1}},\mathrm{ID}|_k)\\ \sigma\leftarrow\mathrm{Sign}(\mathrm{mpk},M,\mathrm{sk}_{\mathrm{ID}|_k})\end{array}\right.\right]=1。$$

### 2.2　安全模型

参考文献[26],本文通过攻击者 $\mathcal{A}$ 与挑战者 $\mathcal{B}$ 之间的交互定义了分层标识签名在适应性选择消息和选择标识攻击下的存在性不可伪造(Existential Un-Forgeability under Adaptive Chosen-Message and chosen-Identity Attacks, EUF-sID-CMA)的安全模型。具体定义如下:

**初始化**。$\mathcal{A}$ 首先声明1个挑战标识 $\mathrm{ID}^*=(\mathrm{ID}_1^*,\mathrm{ID}_2^*,\cdots,\mathrm{ID}_m^*)$ $(1<m\leqslant n)$。

**系统建立**。给定安全参数 $\lambda$,挑战者B运行Setup算法,生成系统的主密钥对(mpk, msk),并将mpk发送给 $\mathcal{A}$。

**询问阶段**。$\mathcal{A}$ 可以发起以下询问:

(1)私钥提取询问。$\mathcal{B}$ 运行KeyGen算法,生成用户 $\mathrm{ID}|_j$ 的私钥 $\mathrm{sk}_{\mathrm{ID}|_j}$,并发送给 $\mathcal{A}$。

(2)签名询问。$\mathcal{B}$ 运行KeyGen算法生成用户 $\mathrm{ID}|_j$ 的签名私钥 $\mathrm{sk}_{\mathrm{ID}|_j}$,接着输入消息 $M$,再运行Sign算法生成签名 $\sigma$,并发送给 $\mathcal{A}$。

**伪造阶段**。$\mathcal{A}$ 输出一个三元组 $(\mathrm{ID}^*,M^*,\sigma^*)$,若其符合以下3个条件,则 $\mathcal{A}$ 获胜。

(1)$\mathcal{A}$ 未曾询问 $\mathrm{ID}^*=(\mathrm{ID}_1^*,\mathrm{ID}_2^*,\cdots,\mathrm{ID}_m^*)$ 中任意一个用户的私钥;

(2)$\sigma^*$ 是 $(\mathrm{ID}^*,M^*)$ 的一个有效分层签名;

(3)$\mathcal{A}$ 未曾询问过 $\mathrm{ID}^*$ 和消息 $M^*$ 的签名。

**定义3**　令攻击者 $\mathcal{A}$ 获胜的概率优势为 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{EUF-sID-CMA}}(\lambda)$,若在任意PPT内对于攻击者 $\mathcal{A}$,$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{EUF-sID-CMA}}(\lambda)$ 都是可以忽略的,则本文方案是EUF-sID-CMA安全的。

## 3　SM9分层标识签名方案

### 3.1　SM9分层标识签名

本文方案在SM9数字签名算法的基础上,借鉴文献[28]的分层标识技术思想,首次提出基于SM9的分层标识签名方案。为表述简洁,方案将 $H_1(\mathrm{ID}\|\mathrm{hid},N)$ 简化为 $H_1(\mathrm{ID})$,故本文方案的具体构造如下:

**参数生成**(Setup)。已知安全参数 $\lambda$ 和层级最大值 $n$,KGC首先选取一个双线性群 $\mathrm{bp}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,N)$,其中 $N$ 为大素数且 $N>2^{\lambda}$,随机选择生成元 $P_1,P_1{}^*,P_2{}^*,\cdots,P_n{}^*\in\mathbb{G}_1$;$P_2\in\mathbb{G}_2$,则有 $P_1=\varphi(P_2)$,选择随机数 $\alpha\in[1,N-1]$,选择两个密码杂凑函数 $H_1,H_2$,分别计算 $\mathbb{G}_2$ 中的元素 $P_{\mathrm{pub}}=\alpha P_2$ 和 $\mathbb{G}_T$ 中的元素 $g=e(P_1,P_{\mathrm{pub}})$,系统的主私钥 $\mathrm{msk}=\alpha$ 和系统主公钥 $\mathrm{mpk}=(\mathrm{bp},P_1,P_1{}^*,P_2^*,\cdots,P_n{}^*,P_2,P_{\mathrm{pub}},g,H_1,H_2,n)$。

**私钥提取**(KeyGen)。已知系统主公钥mpk和第 $k$ 层用户标识 $\mathrm{ID}|_k=(\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_k)$,第 $k-1$ 层用户利用其私钥 $\mathrm{sk}_{\mathrm{ID}|_{k-1}}=(d_1',d_2',d_k',d_{k+1}',\cdots,d_n')$ 并选取随机数 $r'\in\mathbb{Z}_N^*$ 生成第 $k$ 层用户的私钥 $\mathrm{sk}_{\mathrm{ID}|_k}$ 过程如下:

(1)当 $k=1$ 时,第1层用户 $\mathrm{ID}|_1=\mathrm{ID}_1$ 的私钥为 $\mathrm{sk}_{\mathrm{ID}|_1}=(d_1^*,d_2^*)=\left(\dfrac{\alpha}{\alpha+H_1(\mathrm{ID}_1)}P_1+r\cdot P_1^*,r\cdot(\alpha+H_1(\mathrm{ID}_1))P_2\right)$。

（2）当 $1<k\leqslant n$ 时，首先第 $k-1$ 层用户的私钥为 $\mathrm{sk}_{\mathrm{ID}|_{k-1}}=(d_1',d_2',d_k',d_{k+1}',\cdots,d_n')$。其中：

$$\begin{aligned}d_1'&=\frac{\alpha}{\alpha+H_1(\mathrm{ID}_1)}P_1+r'\cdot\left(P_1^*+H_1(\mathrm{ID}_2)P_2^*\right.\\&\quad\left.+\cdots+H_1(\mathrm{ID}_{k-1})P_{k-1}^*\right)\\d_2'&=r'\cdot\left(\alpha+H_1(\mathrm{ID}_1)\right)P_2\\d_k'&=r'\cdot P_k^*\\d_{k+1}'&=r'\cdot P_{k+1}^*\\&\vdots\\d_n'&=r'\cdot P_n^*。\end{aligned}$$

其次，第 $k-1$ 层用户选取随机数 $t\in\mathbb{Z}_N^*$，计算 $r=r'+t\in\mathbb{Z}_N^*$。其具体私钥更新计算过程如下：

$$\begin{aligned}d_1&=\left(d_1'+H_1(\mathrm{ID}_k)\cdot d_k'+t\cdot\left(P_1^*+H_1(\mathrm{ID}_2)P_2^*+\cdots+H_1(\mathrm{ID}_k)P_k^*\right)\right)\\&=\frac{\alpha}{\alpha+H_1(\mathrm{ID}_1)}P_1+r\cdot\left(P_1^*+H_1(\mathrm{ID}_2)P_2^*+\cdots+H_1(\mathrm{ID}_k)P_k^*\right)\\d_2&=d_2'+t\cdot\left(P_{\mathrm{pub}}+H_1(\mathrm{ID}_1)P_2\right)=r\cdot\left(\alpha+H_1(\mathrm{ID}_1)\right)P_2\\d_{k+1}&=d_{k+1}'+t\cdot P_{k+1}^*=r\cdot P_{k+1}^*\\d_{k+2}&=d_{k+2}'+t\cdot P_{k+2}^*=r\cdot P_{k+2}^*\\&\vdots\\d_n&=d_n'+t\cdot P_n^*=r\cdot P_n^*。\end{aligned}$$

最后，输出第 $k$ 层用户私钥为 $\mathrm{sk}_{\mathrm{ID}|_k}=(d_1,d_2,d_{k+1},d_{k+2},\cdots,d_n)$。

**签名生成**(Sign)。令待签名的消息为 $M$，签名者的标识为 $\mathrm{ID}|_k$，签名私钥为 $\mathrm{sk}_{\mathrm{ID}|_k}$，签名者随机选取 $s\in\mathbb{Z}_N^*$，令 $w=g^s$，分别计算 $\sigma_1=H_2(M\|w,N),\sigma_2=(s-\sigma_1)d_1$，$\sigma_3=(s-\sigma_1)d_2$，最后输出对消息 $M$ 的分层签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$。

**签名验证**(Verify)。已知系统主公钥 mpk、消息 $M$ 及其签名 $\sigma'=(\sigma_1',\sigma_2',\sigma_3')$，验证者首先计算 $P'=P_{\mathrm{pub}}+H_1(\mathrm{ID}_1)P_2,Q'=P_1^*+H_1(\mathrm{ID}_2)P_2^*+\cdots+H_1(\mathrm{ID}_k)P_k^*$；紧接着令 $A=e(\sigma_2',P'),B=e(Q',\sigma_3')$，再令 $w'=\frac{A}{B}g^{\sigma_1'}$；最后验证 $H_2(M\|w',N)=\sigma_1$ 是否成立，若成立则验证成功，输出 accept；否则验证失败，输出 reject。

### 3.2 正确性分析

假设 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$ 是消息 $M$ 的正确分层签名值，对应签名者的标识为 $\mathrm{ID}|_k=(\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_k)$ 且签名私钥为 $\mathrm{sk}_{\mathrm{ID}|_k}=(d_1,d_2,d_{k+1},d_{k+2},\cdots,d_n)$，根据签名生成算法和签名验证算法，则有

$$\begin{aligned}w'&=\frac{e(s-\sigma_1')\left(\frac{\alpha}{\alpha+H_1(\mathrm{ID}_1)}P_1+r\cdot\left(P_1^*+H_1(\mathrm{ID}_2)P_2^*+\cdots+H_1(\mathrm{ID}_k)P_k^*\right),\left(\alpha+H_1(\mathrm{ID}_1)\right)P_2\right)}{e\left(P_1^*+H_1(\mathrm{ID}_2)P_2^*+\cdots+H_1(\mathrm{ID}_k)P_k^*,(s-\sigma'_1)\cdot r\cdot\left(\alpha+H_1(\mathrm{ID}_1)\right)P_2\right)}g^{\sigma_1'}\\&=e\left(\frac{\alpha}{\alpha+H_1(\mathrm{ID}_1)}P_1,\left(\alpha+H_1(\mathrm{ID}_1)\right)P_2\right)^{(s-\sigma_1')}g^{\sigma_1'}\\&=e(\alpha P_1,P_2)^{(s-\sigma_1')}g^{\sigma_1'}\\&=g^s=w。\end{aligned}$$

由 $w'=w$ 可得，$H_2(M\|w',N)=\sigma_1$ 成立，验证成功，故方案的正确性成立。

### 3.3 安全性分析

本节分析基于国密 SM9 分层标识签名方案的安全性，本文方案的安全性基于 $(q,n)$-SDH 问题，并在随机谕言机模型下给出了方案的安全性证明。

**定理 1** 令 $H_1,H_2$ 为随机谕言机，如果 $(q,n)$-SDH 假设成立，则本文方案是 EUF-sID-CMA 安全的。

**证明** 假设存在攻击算法 $\mathcal{A}$ 在询问 $q_{H_1}$ 次随机预言机后，能以不可忽略的概率 $\varepsilon$ 伪造签名，则可构造一个模拟算法 $\mathcal{B}$ 通过与 $\mathcal{A}$ 交互，以不可忽略的概率 $\frac{\varepsilon}{q_{H_1}}$ 求解 $(q,n)$-SDH 问题。$\mathcal{B}$ 以 $(q,n)$-SDH 问题的实例 $\left(c,P,bP,aP,a^2P,\cdots,a^qP,\frac{1}{(a+c)^2}P,\frac{1}{(a+c)^3}P,\cdots,\frac{1}{(a+c)^n}P,Q,bQ,aQ,a^2Q,\cdots,a^{n+1}Q\right)$ 为输入，目标是找到一对二元组 $\left(c,\frac{1}{c+a}P\right)$，其中 $c\in\mathbb{Z}_N^*$，$\mathcal{B}$ 为挑战者，$\mathcal{A}$ 为攻击者。

**初始化**。攻击者 $\mathcal{A}$ 输出挑战用户标识 $\mathrm{ID}^*=(\mathrm{ID}_1^*,\mathrm{ID}_2^*,\cdots,\mathrm{ID}_m^*)(1<m\leqslant n)$。

**系统建立**。挑战者 $\mathcal{B}$ 首先设系统主私钥 $\mathrm{msk}=\alpha=a$，其中 $a$ 未知，接着执行以下步骤。

（1）随机选取两两不同的数 $w_1,w_2,\cdots,w_q\in\mathbb{Z}_N^*$，设为第 1 层除 $\mathrm{ID}_1^*$ 外所有标识的哈希值，并定义多项式

$$f(a)=(a+w_1)(a+w_2)\cdots(a+w_q)\bmod p$$

（2）接着计算群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 中的元素 $P_1=f(a)P,P_2=Q,P_{\mathrm{pub}}=aP_2=aQ$，其中 $P=\varphi(Q)$。

（3）令 $x^*=c=H_1(\mathrm{ID}_1^*)$，选取各不同的随机数 $x_2^*,x_3^*,\cdots,x_m^*\in\mathbb{Z}_N^*$，将 $x_i^*$ 设为 $H_1(\mathrm{ID}_i^*)$，对于任意的 $i\in[2,n]$，可计算：

$$P_i^*=x_iP+\frac{y_i}{(a+x^*)^{n+2-i}}P。$$

（4）紧接着随机选取 $2n-1$ 个两两不同的随机数

$x_1,x_2,\cdots,x_n,y_2,y_3,\cdots,y_n\in\mathbb{Z}_N^*$并计算:

$$P_1^*=x_1(a+x^*)P-\sum_{i=2}^{m}x_i^*P_i^*,g=e(P_1,P_{\text{pub}})。$$

最后输出系统主公钥$\text{mpk}=(\text{bp},P_1,P_1{}^*,P_2^*,\cdots,P_n{}^*,P_{\text{pub}},P_2,g,H_1,H_2,n)$,其中密码杂凑函数$H_1,H_2$可以看作是由$\mathcal{B}$掌握的随机谕言机。

**询问阶段**。在此阶段攻击者$\mathcal{A}$可以进行$H_1$询问、$H_2$询问、私钥提取询问以及签名询问。

(1)$H_1$询问。$\mathcal{B}$为$H_1$询问生成初始化为空的Hash列表$L_1$,并以二元组$(\text{ID}_i,h_i)$的形式存储表中元素。已知询问的标识为$\text{ID}_i$,若被询问标识已存在于列表$L_1$中,则$\mathcal{B}$返回相应的$h_i$,否则,按以下流程回复$\mathcal{A}$。

(a)当$\text{ID}_i$为第1层标识时:

如果$\text{ID}_i=\text{ID}_1^*$,设$h_i=H_1(\text{ID}_1^*)=x^*=c$,将$h_i$发送给$\mathcal{A}$并以二元组$(\text{ID}_i,h_i)$更新列表$L_1$;如果$\text{ID}_i\neq\text{ID}_1^*$,设$h_i=H_1(\text{ID}_i)=w_i$,将$h_i$发送给$\mathcal{A}$并以二元组$(\text{ID}_i,h_i)$更新列表$L_1$。

(b)当ID不为第1层标识时:

如果$\text{ID}_i=\text{ID}_j^*,j\in[2,m]$,设$h_i=H_1(\text{ID}_j^*)=x_j^*$,将$h_i$发送给$\mathcal{A}$并以二元组$(\text{ID}_i,h_i)$更新列表$L_1$;如果$\text{ID}_i\neq\text{ID}_j^*,j\in[2,m]$,随机选取$z_i=\mathbb{Z}_N^*$,设$h_i=H_1(\text{ID}_i)=z_j$将$h_i$发送给$\mathcal{A}$并以二元组$(\text{ID}_i,h_i)$更新列表$L_1$。

(2)$H_2$询问。已知二元组$(M_i,w_i)$,$\mathcal{B}$为$H_2$询问生成初始化为空的Hash列表$L_2$,并以三元组$(M,w,\sigma_1)$的形式存储表中元素。若询问的$(M_i,w_i)$在列表$L_2$中,则$\mathcal{B}$返回相应的$\sigma_{1i}$。否则,从$\mathbb{Z}_N^*$中随机选取一个元素$\sigma_{1i}$,设$H_2(M_i,w_i)=\sigma_{1i}$,将$\sigma_{1i}$发送给$\mathcal{A}$并以三元组$(M_i,w_i,\sigma_{1i})$更新列表$L_2$。

首先在私钥询问和签名询问阶段,我们令询问标识为$\text{ID}|_j=(\text{ID}_1,\text{ID}_2,\cdots,\text{ID}_j)$,并要求$\text{ID}|_j\neq\text{ID}^*$且不是$\text{ID}^*$的上一层标识,其中$1<j\leqslant n$。

(1)私钥询问。

(a)$\text{ID}_1\neq\text{ID}_1^*$时,$H_1(\text{ID}_1)=w_i(i=1,2,\cdots,q)$,由上述系统参数可得,$f(a)=(a+w_1)(a+w_2)\cdots(a+w_q)\bmod p$,因此,可以通过已知困难问题的给定实例,有效求得$\dfrac{\alpha}{\alpha+H_1(\text{ID}_1)}P_1$的取值,并据此由私钥生成算法得到合法的私钥,即

$$\frac{\alpha}{\alpha+H_1(\text{ID}_1)}P_1=\frac{a(a+w_1)(a+w_2)\cdots(a+w_q)}{a+w_i}P。$$

(b)$\text{ID}_1=\text{ID}_1^*$时,由于$\text{ID}|_j\neq\text{ID}^*$且不是$\text{ID}^*$的上一层标识,设第一个不相等的标识分量索引为$l\in[2,j]$,则有$\text{ID}_l\neq\text{ID}_l^*$,使得

$$\frac{\alpha}{\alpha+H_1(\text{ID}_1^*)}P_1=\frac{\alpha f(a)}{\alpha+H_1(\text{ID}_1^*)}P=f(a)P+\frac{W}{a+x^*}P。$$

其中,$f(a)=(a+w_1)(a+w_2)\cdots(a+w_q)\bmod p$,$W=-x^*$,又因为$(\text{ID}_1,\text{ID}_2,\cdots,\text{ID}_{l-1})=(\text{ID}_1^*,\text{ID}_2^*,\cdots,\text{ID}_{l-1}^*)$对任意$i\in[2,n]$,均有$P_i^*=x_iP+\dfrac{y_i}{(a+c)^{n+2-i}}P$,可得

$$\begin{aligned}
&P_1^*+H_1(\text{ID}_2)P_2^*+H_1(\text{ID}_3)P_3^*+\cdots+H_1(\text{ID}_j)P_j^*\\
&=x_1(a+x^*)P-\sum_{i=2}^{m}x_i^*P_i^*+z_2P_2^*+z_3P_3^*+\cdots+z_jP_j^*\\
&=x_1(a+x^*)P-\sum_{i=2}^{m}x_i^*P_i^*+x_2^*P_2^*+x_3^*P_3^*+\cdots+x_{l-1}^*P_{l-1}^*\\
&\quad+z_lP_l^*+\cdots+z_jP_j^*\\
&=x_1(a+x^*)P-\sum_{i=k}^{m}x_i^*P_i^*+z_lP_l^*+\cdots+z_jP_j^*\\
&=x_1(a+x^*)P+XP+\frac{Y_l}{(a+c)^{n+2-l}}P+\cdots+\frac{Y_{\max(m,j)}}{(a+c)^{n+2-\max(m,j)}}P。
\end{aligned}$$

接着$\mathcal{B}$选取$z\in\mathbb{Z}_N^*$,令$r=z-\dfrac{W}{Y_l}(a+x^*)^{(2+n-l)-1}$,并计算:

$$\begin{aligned}
d_1&=\frac{\alpha}{\alpha+H_1(\text{ID}_1^*)}P_1+r\cdot(P_1^*+H_1(\text{ID}_2)P_2^*+\cdots+H_1(\text{ID}_j)P_j^*)\\
&=f(a)P+\frac{W}{a+x^*}P+\left(z-\frac{W}{Y_l}(a+x^*)^{(2+n-l)-1}\right)\cdot(x_1(a+x^*)P\\
&\quad+XP+\frac{Y_l}{(a+c)^{n+2-l}}P+\cdots+\frac{Y_{\max(m,j)}}{(a+c)^{n+2-\max(m,j)}}P)\\
&=f(a)P+z\cdot(x_1(a+x^*)P+XP+\frac{Y_l}{(a+c)^{n+2-l}}P+\cdots\\
&\quad+\frac{Y_{\max(m,j)}}{(a+c)^{n+2-\max(m,j)}}P)-\frac{x_1W}{Y_l}(a+x^*)^{(2+n-l)}P\\
&\quad-\frac{XW}{Y_l}(a+x^*)^{(2+n-l)-1}P-\frac{Y_{l+1}W}{Y_l}P-\frac{Y_{l+2}W}{Y_l}(a+x^*)P\\
&\quad-\cdots-\frac{Y_{\max(m,j)}W}{Y_l}(a+x^*)^{(\max(m,j)-l-1)}P,\\
d_2&=r\cdot(a+H_1(\text{ID}_1^*))P_2\\
&=\left(z-\frac{W}{Y_l}(a+x^*)^{(2+n-l)-1}\right)\cdot(a+x^*)Q\\
&=z(a+x^*)Q-\frac{W}{Y_l}(a+x^*)^{(2+n-l)}Q。
\end{aligned}$$

对于$i\in[j+1,n]$,计算:

$$\begin{aligned}
d_i&=r\cdot P_i^*\\
&=\left(z-\frac{W}{Y_l}(a+x^*)^{(2+n-l)-1}\right)\cdot\left(x_iP+\frac{y_i}{(a+x^*)^{n+2-i}}P\right)\\
&=z\cdot\left(x_iP+\frac{y_i}{(a+c)^{n+2-i}}P\right)-\frac{x_iW}{Y_l}(a+x^*)^{(2+n-l)-1}P\\
&\quad-\frac{y_iW}{Y_l}(a+x^*)^{i-l-1}P。
\end{aligned}$$

从上面给定的实例计算可得$\text{sk}_{\text{ID}|_j}$为正确的私钥,最后,$\mathcal{B}$发送私钥$\text{sk}_{\text{ID}|_j}=(d_1,d_2,d_{j+1},d_{j+2},\cdots,d_n)$给$\mathcal{A}$。

(2)签名询问。

(a)$\mathrm{ID}_1 \neq \mathrm{ID}_1^*$时,挑战者$\mathcal{B}$可用上述方案中的私钥提取算法获取其对应的签名私钥,并根据签名生成算法生成有效的签名。

(b)$\mathrm{ID}_1 = \mathrm{ID}_1^*$时,挑战者$\mathcal{B}$首先在$L_1$列表中查询$h_i$对应的值为$x^*$,并计算$P' = h_i P_2 + P_{\mathrm{pub}} = (x^* + a)Q$,然后随机选择$\sigma_1 \in \mathbb{Z}_N^*$,$\sigma_2 \in \mathbb{G}_1$,$\sigma_3 \in \mathbb{G}_2$,并计算$w = \dfrac{e(\sigma_2, P')}{e(Q', \sigma_3)} g^{\sigma_1}$,最后,$\mathcal{B}$将$(M, w)$添加到列表$L_2$,并定义$H_2(M \| w, N) = \sigma_1$。若$(M, w)$被询问过,则$\mathcal{B}$输出模拟失败。

**伪造阶段**:$\mathcal{A}$输出关于$M^*, \mathrm{ID}^*$的1个有效签名$\sigma^*$,其中$\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*)$。由文献[31]分叉引理可知,若$\mathcal{A}$能在未知相应签名私钥的情况下成功伪造签名,则存在一个图灵机$\mathcal{A}'$通过$\mathcal{A}$的帮助,以相同的输入$(\mathrm{mpk}, M^*, w^*, \mathrm{ID}^*)$,在时间$t'$内输出两个有效的伪造签名$(M^*, w^*, \sigma_1^*, \sigma_2^*, \sigma_3^*)$和$(M^*, w^*, \sigma'^*_1, \sigma'^*_2, \sigma'^*_3)$其中$\sigma_1^* \neq \sigma'^*_1, \sigma_2^* \neq \sigma'^*_2, \sigma_3^* \neq \sigma'^*_3$,且2个有效的伪造签名满足以下等式:

$$\frac{e(P', \sigma_2^*)}{e(\sigma_3^*, Q')} g^{\sigma_1^*} = \frac{e(P', \sigma'^*_2)}{e(\sigma'^*_3, Q')} g^{\sigma'^*_1}。$$

化简可得

$$\begin{aligned} & e((\alpha + x^*)P_2, \sigma_2^* - \sigma'^*_2) \\ &= e(\sigma_3^* - \sigma'^*_3, x_1(\alpha + x^*)P_1) e(P_1, P_2)^{\alpha(\sigma'^*_1 - \sigma_1^*)} \\ &\quad \cdot e((\alpha + x^*)P_2, \alpha^{-1}(\sigma'^*_1 - \sigma_1^*)^{-1}(\sigma_2^* - \sigma'^*_2)) \\ &= e(\sigma_3^* - \sigma'^*_3, x_1(\alpha + x^*)P_1) e(P_1, P_2)。 \end{aligned}$$

令$Y_1^* = \dfrac{\sigma_2^* - \sigma'^*_2}{\sigma'^*_1 - \sigma_1^*} = d_1$,根据等式有

$$\begin{aligned} Y_1^* &= \frac{\alpha}{\alpha + H_1(\mathrm{ID}_1^*)} P_1 + r \cdot (P_1^* + H_1(\mathrm{ID}_2^*) P_2^* \\ &\quad + \cdots + H_1(\mathrm{ID}_m^*) P_k^*) \\ &= \frac{\alpha}{\alpha + H_1(\mathrm{ID}_1^*)} P_1 + r \cdot (x_1(a + x^*)P_1 \\ &\quad - \sum_{i=2}^{m} x_i^* P_i^* + x_2^* P_2^* + \cdots + x_m^* P_k^*)。 \end{aligned}$$

令$Y_2^* = \dfrac{\sigma_3^* - \sigma'^*_3}{\sigma'^*_1 - \sigma_1^*} = d_2$,根据等式有$Y_2^* = r \cdot (\alpha + H_1(\mathrm{ID}_1^*))P_2$,又因为:

$$\frac{\alpha f(\alpha)}{\alpha + x^*} + r \cdot x_1(\alpha + x^*) = \frac{\gamma}{\alpha + x^*} + \sum_{i=0}^{k} \gamma_i \alpha^i + r \cdot x_1(\alpha + x^*),$$

$$P_1 = f(a)P。$$

其中,$\gamma, \gamma_i$是可求系数且$\gamma \neq 0$,最后计算:

$$\begin{aligned} X^* &= \frac{1}{\gamma}\left(Y_1^* - \sum_{i=0}^{k} \gamma_i \varphi(\alpha^i Q) - x_1 \varphi(Y_2^*)\right) \\ &= \frac{1}{\alpha + x^*} P。 \end{aligned}$$

故输出$(x^*, X^*)$作为$(q, n)$-SDH问题实例的解。

综上所述,在签名伪造阶段,若$\mathcal{A}$未询问过挑战标识的签名私钥且输出伪造签名,此事发生的概率为$\dfrac{1}{q_{H_1}}$,即$\mathcal{B}$能成功完成模拟的概率为$\dfrac{1}{q_{H_1}}$。因此,若$\mathcal{A}$能以不可忽略的概率$\varepsilon$成功伪造签名,则$\mathcal{B}$就可以以不可忽略的概率$\dfrac{\varepsilon}{q_{H_1}}$成功求解$(q, n)$-SDH问题,其中$q_{H_1}$为$H_1$询问的次数。证毕

## 4 基于SM9分层签名的车联网身份认证方案

车联网技术的迭代升级,正强力驱动着智能交通系统的发展[32-33],使其战略意义与日俱增。尤其在新能源汽车广泛推广的背景下,车辆智能化水平不断提升,能够通过自组织网络实现碰撞预警、导航定位、自动驾驶及智能泊车等服务。然而,在这一过程中,存在恶意用户假冒车辆身份或利用通信信息对车辆进行跟踪等攻击行为,导致车辆隐私信息泄露甚至被窃取的风险。因此,身份认证在车联网中成为一个关键的安全问题。

传统的身份认证机制通常依赖于中心化架构,容易引发单点故障问题。一旦中心节点遭受攻击,整个认证体系的安全将面临严重威胁。此外,在车流量较大时,中心认证系统面临巨大的计算压力,认证效率显著下降,难以满足高速移动环境下车联网对实时性和可靠性的要求,甚至可能引发网络拥堵,进而影响行车安全。

针对这些问题,根据本文提出的基于SM9的分层标识签名方案,设计了一种轻量级、去中心化的车联网身份认证方案,能够有效地确保车辆与车辆之间通信认证的安全性和高效性,其方案核心流程如图1所示。

该车联网身份认证核心方案包含5个实体,分别是:

国家交通管理中心(根KGC):负责生成系统主密钥对(mpk, msk),根据下级部门的标识ID来生成和分发下级部门的私钥。

省级交管部门(域KGC):负责注册部门ID,再根据路侧单元和车辆的唯一信息标识来生成和分发路侧单元和车辆的私钥。

路测单元RSU:负责注册单元ID,收集环境信息并对其进行签名和转发。

$\mathrm{A}_{车}$车载单元:负责注册车辆ID,收集行驶信息并对其进行签名与转发,接收和验证签名。

$\mathrm{B}_{车}$车载单元:负责注册车辆ID,接收签名并对其

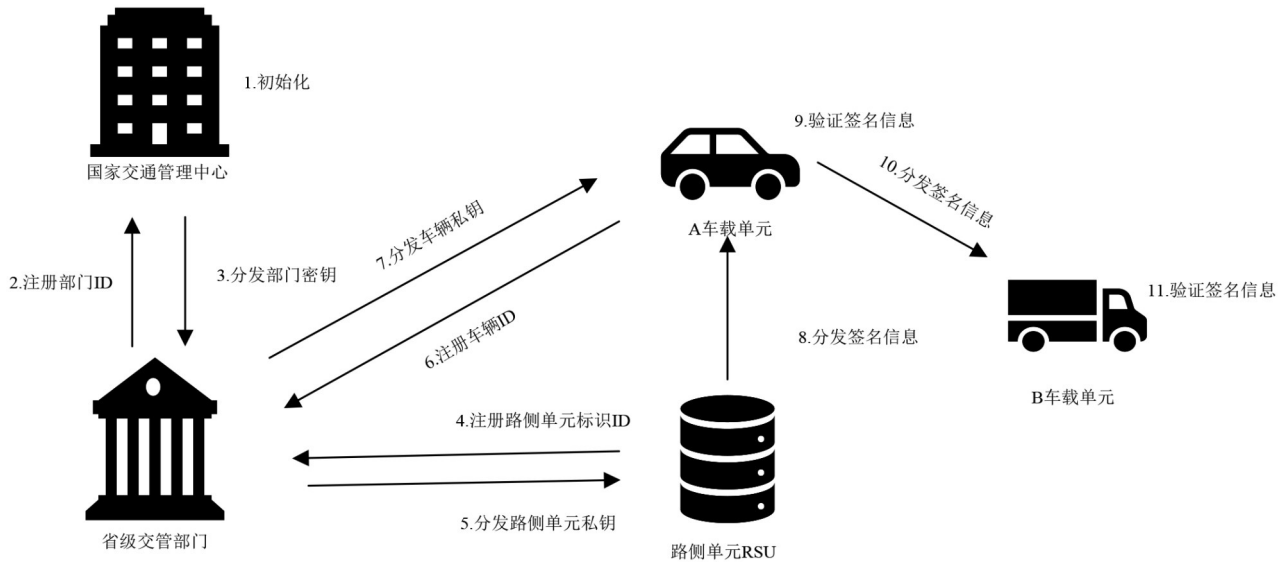



图1　车联网身份认证核心流程

Figure 1　Core process of vehicle network identity authentication

进行验证。

具体的核心认证流程描述如下:

(1)国家交通管理中心执行Setup算法,生成系统的主密钥对(mpk, msk),公开系统主公钥mpk,保密存储系统主私钥msk,完成系统初始化。

(2)省级交管部门向国家交通管理中心提交自己的省份标识$ID|_s$以请求部门私钥。

(3)国家交通管理中心执行KeyGen算法,生成省级交管部门的私钥$sk_{ID|_s}$,并通过安全信道发送给省级交管部门。

(4)路侧单元RSU向省级交管部门提交自己的身份标识$ID|_{RSU}$以请求路侧单元私钥$sk_{ID|_{RSU}}$。

(5)省级交管部门验证路侧单元RSU的身份标识并根据本部门私钥$sk_{ID|_s}$执行KeyGen算法,生成路侧单元的私钥$sk_{ID|_{RSU}}$并通过可信信道发送给路侧单元RSU。

(6)$A_{车}$(或$B_{车}$)车载单元向省级交管部门提交自身的唯一标识(车牌号或者VIN(车辆识别码))以请求$A_{车}$(或$B_{车}$)车载单元的私钥$sk_{ID|_{A_{车}}}$(或$sk_{ID|_{B_{车}}}$)。

(7)省级交管部门验证$A_{车}$(或$B_{车}$)车载单元的身份并根据本部门私钥$sk_{ID|_s}$执行KeyGen算法,生成$A_{车}$(或$B_{车}$)车载单元的私钥$sk_{ID|_{A_{车}}}$(或$sk_{ID|_{B_{车}}}$)并通过可信信道发送给$A_{车}$(或$B_{车}$)车载单元。

(8)路侧单元现场收集的信息(天气,红绿灯信号等),使用私钥$sk_{ID|_{RSU}}$给收集到的信息$M_1$进行签名得到签名值$\sigma_1$,并将签名值$\sigma_1$发送给$A_{车}$车载单元。

(9)$A_{车}$车载单元根据收到的消息$M_1$和相应签名$\sigma_1$,使用Verify算法进行验证,若验证通过则接收消息,否则丢弃消息。

(10)$A_{车}$车载单元再根据行驶中收集到的数据(刹车,事故)打包生成消息$M_2$,同时使用私钥$sk_{ID|_{A_{车}}}$给消息进行签名得到签名值$\sigma_2$,将签名值$\sigma_2$发送给$B_{车}$车载单元。

(11)$B_{车}$车载单元根据收到的消息$M_2$和相应签名$\sigma_2$使用Verify算法验证签名,若成功验证则保留消息,否则丢弃消息。

方案用分层签名实现了去中心化认证,解决了车联网身份认证中的单点故障问题;同时方案支持无证书认证,验证签名信息仅需路侧单元或车载单元的身份标识和系统主公钥,有效降低了车联网身份认证中的存储开销。根KGC不参与车辆认证,降低了密钥泄露的风险;省级KGC分区域管理车辆,实现路侧单元和车辆的注册和分发私钥,有效缓解中心化系统的计算压力;同时随着分层层数的增加,系统的签名生成时间总体趋于不变,故在分层层数足够多的情况下,系统的计算开销优势明显。最后,该方案通过SM9分层标识签名实现了轻量级、高安全和高效率的车联网身份认证,适用于大规模智能交通系统。

## 5　方案性能分析

### 5.1　计算开销分析

本节将分析分层签名方案的计算开销,分析对比本文方案和基于双线性对的分层标识签名文献[4, 6, 8, 10]方案和原SM9数字签名[11]在计算开销上的

差别。首先比较私钥提取算法、签名生成算法和签名验证算法的计算开销。参数生成算法可由根KGC提前完成，不影响系统整体的效率，故我们就不作开销对比，对比结果如表2所示。$n$为系统最大层级数，$k$为系统当前层级数，BP为双线性运算，$E_t$为群$\mathbb{G}_T$中的指数运算，SM为群$\mathbb{G}$中的标量乘运算，$SM_1$和$SM_2$分别为群$\mathbb{G}_1$和$\mathbb{G}_2$中的标量乘运算，同时省略掉其中耗时很短的哈希运算、模逆运算和模乘运算等。

**表2 签名方案的计算开销对比**

Table 2 Comparative analysis of computational cost for signature schemes

| 方案 | 私钥提取 | 签名生成 | 签名验证 |
|---|---|---|---|
| 文献[4] | $k$SM | $(k+1)$SM | $(k+2)$BP |
| 文献[6] | $(3k+1)$SM | $(k+2)$SM | $(k+2)$BP+$(k+1)$SM |
| 文献[8] | $(n+3)$SM | $(2k+8)$SM | 6BP+$E_t$+2$k$SM |
| 文献[10] | $(n+3)$SM | $(k+2)$SM | 4BP+2$k$SM |
| 原SM9 | $SM_1$ | $SM_1+E_t$ | $SM_2+E_t$+BP |
| 本文 | $(n+1)SM_1+2SM_2$ | $E_t$ | $2BP+E_t+kSM_1+2SM_2$ |

如表2所示，本文方案的私钥提取算法需要线性个群$\mathbb{G}_1$中的标量乘法运算，其他几个分层签名文献的方案私钥提取算法需要线性个群$\mathbb{G}$中的标量乘运算；对于签名生成算法，本文方案仅需1个群$\mathbb{G}_T$中的指数运算，其他几个文献的方案需要线性个群$\mathbb{G}$中的标量乘运算；对于签名验证算法，本文方案仅需要2个双线性对运算，文献[4]方案和文献[6]方案则需要$k+2$个双线性对运算，文献[8]方案和文献[10]方案分别需要6个和4个双线性对运算。因为双线性对运算时间远大于群中的标量乘运算时间和群中的指数运算时间，故在签名生成与验证阶段，本文方案具备一定的性能优势。

为了表2对比的结果更加直观，本文使用C++编程语言和GmssL库，在2.50 GHz的16核心32线程的AMD Ryzen 97 945HX with Randeon Graphics处理器，Windows 11操作系统和16 GB内存的lenovo笔记本电脑上使用Microsoft Visual Studio 2026编辑器进行实验仿真，采用256 bit的BN曲线为椭圆曲线，曲线方程为$y^2=x^3+3$，分别在系统当前层数$k$为2、4、6、8、10的情况下测试了方案中签名生成算法、签名验证算法以及总体的计算开销，其中实验数据取自给定当前层数的情况下100次实验结果的平均值，实验结果如图2~4所示。

图2为不同签名方案的签名生成计算开销对比图，实验结果表明本文方案的签名生成时间略优于原SM9方案，且明显优于其他4个分层签名文献的方案。本文方案的签名生成时间与$k$无关，呈常量级，而其他4个文献的方案签名生成时间随着$k$的增加而增加。随着系统当前层数$k$的增加，本文方案的签名生成时间开销优势更为明显。当系统当前层数$k$为2~10的情况下，本文方案的签名生成时间约为2.24 ms，比签名生成计算开销最优的文献[4]方案提升0.03~2.79倍，故本文方案的签名生成计算开销存在一定的性能优势。

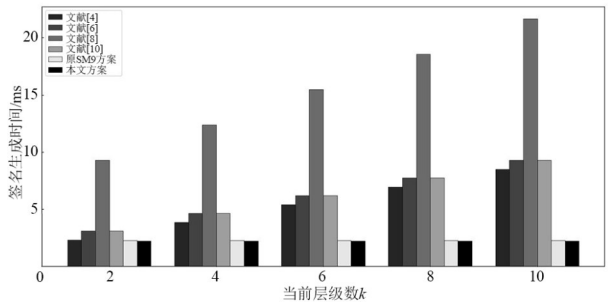



图2 签名生成计算开销对比

Figure 2 Signature generation computational overhead comparison

图3为不同签名方案的签名验证计算开销对比图，实验结果表明本文方案的签名验证时间高于原SM9签名方案，但明显优于其他4个分层签名文献的方案。且随着系统当前层数$k$的增加，本文方案的签名生成时间开销优势更为明显。在系统当前层数$k$为2~10的情况下，本文方案的签名验证时间约为36.08 ms，比签名验证时间开销最优的文献[4]方案和文献[10]方案提升0.87~1.27倍，故本文方案的签名验证计算开销存在一定的性能优势。

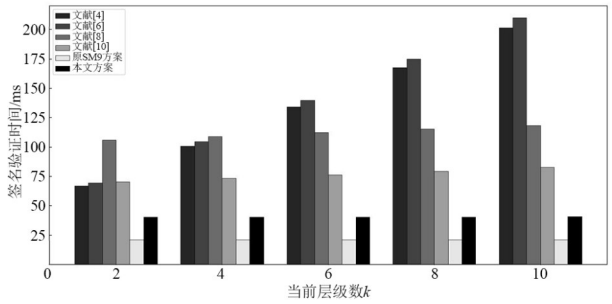
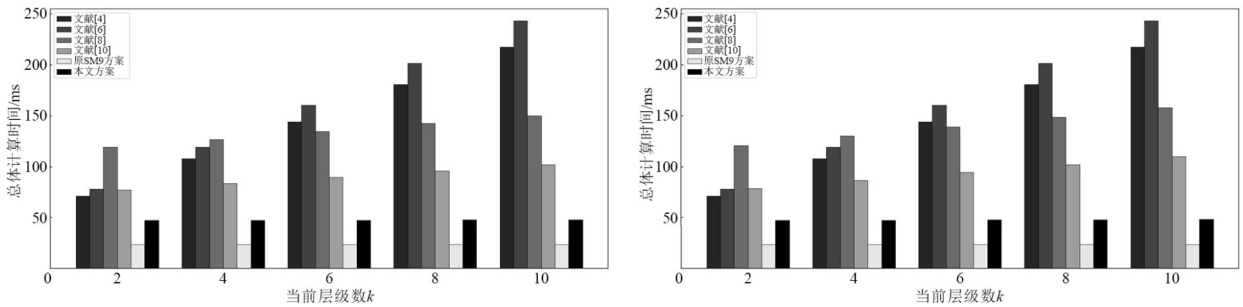



图3 签名验证计算开销对比

Figure 3 Signature verification computational overhead comparison

图4(a)和图4(b)为不同分层签名方案分别在$n=k$和$n=2k$情况下的总体计算开销对比图，结果表明随着$k$的增加，本文方案的总体计算时间略高于原SM9签名方案，但明显小于其他4个分层签名文献的方案。且随着系统当前层数$k$的增加，本文方案的总体计算生成时间开销优势更为明显，故本文方案的总体计算开销存在一定的性能优势。




(a) $n=k$时总体计算开销　　(b) $n=2k$时总体计算开销

(a) Total computational cost when $n=k$　　(b) Total computational cost when $n=2k$

图4　总体计算开销对比

Figure 4　Total computational cost

### 5.2　存储开销分析

接着就是比较系统公钥、用户私钥和签名的存储开销,对比结果如表3所示。$|\mathbb{G}|$为对称群$\mathbb{G}$中的元素大小,$|\mathbb{G}_1|$和$|\mathbb{G}_2|$分别为非对称群$\mathbb{G}_1$和$\mathbb{G}_2$中元素的二进制比特长度,$|\mathbb{G}_T|$为群$\mathbb{G}_T$中元素的二进制比特长度,$|\mathbb{Z}_N|$为群$\mathbb{Z}_N$中元素的二进制比特长度。我们以256比特的BN曲线为例,其中$|\mathbb{G}|=|\mathbb{G}_1|=512$ bit,$|\mathbb{G}_2|=1\ 024$ bit,$|\mathbb{G}_T|=3\ 072$ bit,$|\mathbb{Z}_N|=256$ bit。显然,本文方案的系统公钥长度高于其他方案。当系统最大层数$n$固定时,本文方案与文献[8]方案和文献[10]方案的用户私钥长度随着系统当前层数$k$的增加而减少,文献[4]方案和文献[6]方案的用户私钥长度随着系统当前层数$k$的增加而增加;其次本文方案的签名长度高于文献[4]方案、文献[10]方案,小于文献[6]方案、文献[8]方案,故得本文方案的系统公钥长度高于其他文献的方案,用户私钥长度和签名长度与其他文献的方案是可比的。

**表3　签名方案的存储开销对比**

Table 3　Comparison of storage overhead for signature schemes

| 方案 | 系统公钥长度 | 用户私钥长度 | 签名长度 |
|---|---|---|---|
| 文献[4] | $2\|\mathbb{G}\|$ | $k\|\mathbb{G}\|$ | $\|\mathbb{G}\|$ |
| 文献[6] | $(n+3)\|\mathbb{G}\|$ | $(k+1)\|\mathbb{G}\|$ | $(k+2)\|\mathbb{G}\|$ |
| 文献[8] | $(n+6)\|\mathbb{G}\|$ | $(n-k+2)\|\mathbb{G}\|$ | $4\|\mathbb{G}\|$ |
| 文献[10] | $(n+6)\|\mathbb{G}\|$ | $(n-k+2)\|\mathbb{G}\|$ | $3\|\mathbb{G}\|$ |
| 原SM9 | $\|\mathbb{G}_1\|+2\|\mathbb{G}_2\|+\|\mathbb{G}_T\|$ | $\|\mathbb{G}_1\|$ | $\|\mathbb{G}_1\|+\|\mathbb{Z}_N\|$ |
| 本文 | $(n+1)\|\mathbb{G}_1\|+2\|\mathbb{G}_2\|+\|\mathbb{G}_T\|$ | $(n-k+1)\|\mathbb{G}_1\|+\|\mathbb{G}_2\|$ | $\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+\|\mathbb{Z}_N\|$ |

图5为不同签名方案的签名存储开销对比,由实验结果可得,本文方案的签名存储开销优于文献[6]方案和文献[8]方案,相比原SM9方案、文献[4]方案和文献[10]方案不具备签名存储开销优势。

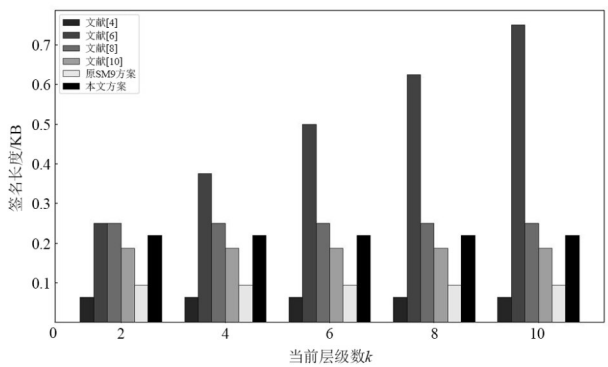



图5　签名存储开销对比

Figure 5　Signature storage overhead comparison

## 6　结束语

为了解决在大规模网络环境中密钥生成中心工作压力繁重,易引发网络拥堵的问题,并推动国产密码技术的应用替代,本文基于国产商用密码SM9数字签名算法,设计了一种高效的SM9分层标识签名方案。并于随机预言机模型中,对方案进行了安全性证明。进一步地,本文将所提方案应用于车联网身份认证场景,构建了一种去中心化的身份认证机制,可有效防范大规模网络环境中车辆隐私信息泄露等问题。通过与现有基于双线性对的分层标识签名方案进行性能对比,结果表明,本文方案在签名生成和验证阶段具有明显的性能优势。具体而言,当系统当前层数$k$为100时,与最优的分层签名方案相比,本文方案的签名生成效率提升约34倍,签名验证效率提升约4.5倍,展现出良好的应用潜力。然而,本方案在存储开销方面略高,因此未来研究将重点探索如何减少分层签名数量,以进一步降低存储成本;本文由于篇幅受限,在考虑应用场景时,仅考虑应用于车联网的身份认证场景中,未来在考虑降低签名方案存储开销的同时,

并将其应用于实体规模更为庞大的区块链场景中。

**参考文献**


[1] Shamir A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology. Berlin, Heidelberg: Springer, 2007: 47-53.

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]//Advances in Cryptology - CRYPTO 2001. Berlin, Heidelberg: Springer, 2001: 213-229.

[3] Horwitz J, Lynn B. Toward hierarchical identity-based encryption[C]//Advances in Cryptology - EUROCRYPT 2002. Berlin, Heidelberg: Springer, 2002: 466-481.

[4] Gentry C, Silverberg A. Hierarchical ID-based cryptography[C]//Advances in Cryptology - ASIACRYPT 2002. Berlin, Heidelberg: Springer, 2002: 548-566.

[5] Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles[C]//Advances in Cryptology - EUROCRYPT 2004. Berlin, Heidelberg: Springer, 2004: 223-238.

[6] Chow S S M, Hui L C K, Yiu S M, et al. Secure hierarchical identity based signature and its application[C]//Information and Communications Security. Berlin, Heidelberg: Springer, 2004: 480-494.

[7] Boneh D, Boyen X, Goh E J. Hierarchical identity based encryption with constant size ciphertext[C]//Advances in Cryptology - EUROCRYPT 2005. Berlin, Heidelberg: Springer, 2005: 440-456.

[8] Yuen H, Wei K. Constant-size hierarchical identity-based signature/signcryption without random oracles[J]. Cryptology ePrint archive, 2005.

[9] Au M H, Liu J K, Yuen T H, et al. Practical hierarchical identity based encryption and signature schemes without random oracles[J]. Cryptology ePrint Archive, 2006.

[10] 吴青, 张乐友, 胡予濮. 标准模型下一种新的基于分级身份的短签名方案[J]. 计算机研究与发展, 2011, 48(8): 1357-1362.
Wu Qing, Zhang Leyou, Hu Yupu. A new construction of short hierarchical identity-based signature in the standard model[J]. Journal of Computer Research and Development, 2011, 48(8): 1357-1362. (in Chinese)

[11] GM/T 0044.1—2016 SM9 标识密码算法 第 1 部分:总则[S].
GM/T 0044.1—2016 Identity-based cryptographic algorithms SM9: Part 1: General[S].

[12] 彭聪, 何德彪, 罗敏, 等. 基于SM9标识密码算法的环签名方案[J]. 密码学报, 2021, 8(4): 724-734.
Peng Cong, He Debiao, Luo Min, et al. An identity-based ring signature scheme for SM9 algorithm[J]. Journal of Cryptologic Research, 2021, 8(4): 724-734. (in Chinese)

[13] 邓浩明, 彭长根, 丁红发, 等. 基于国密SM9算法的门限环签名方案[J]. 计算机技术与发展, 2022, 32(12): 95-102.
Deng Haoming, Peng Changgen, Ding Hongfa, et al. A threshold ring signature scheme based on GM SM9 algorithm[J]. Computer Technology and Development, 2022, 32(12): 95-102. (in Chinese)

[14] 安浩杨, 何德彪, 包子健, 等. 基于SM9数字签名的环签名及其在区块链隐私保护中的应用[J]. 计算机研究与发展, 2023, 60(11): 2545-2554.
An Haoyang, He Debiao, Bao Zijian, et al. Ring signature based on the SM9 digital signature and its application in blockchain privacy protection[J]. Journal of Computer Research and Development, 2023, 60(11): 2545-2554. (in Chinese)

[15] 王伊婷, 万武南, 张仕斌, 等. 基于SM9算法的可链接环签名方案[J]. 计算机应用, 2024, 44(12): 3709-3716.
Wang Yiting, Wan Wunan, Zhang Shibin, et al. Linkable ring signature scheme based on SM9 algorithm[J]. Journal of Computer Applications, 2024, 44(12): 3709-3716. (in Chinese)

[16] 谢振杰, 张耀, 杨启超, 等. 基于国密算法SM9的环签名方案[J]. 计算机科学, 2025, 52(12): 384-390.
Xie Zhenjie, Zhang Yao, Yang Qichao, et al. Ring signature scheme based on domestic cryptographic algorithm SM9[J]. Computer Science, 2025, 52(12): 384-390. (in Chinese)

[17] 谢振杰, 尹小康, 蔡瑞杰, 等. 基于国密算法SM9的可追踪环签名方案[J]. 通信学报, 2025, 46(3): 199-211.
Xie Zhenjie, Yin Xiaokang, Cai Ruijie, et al. Traceable ring signature scheme based on domestic cryptographic algorithm SM9[J]. Journal on Communications, 2025, 46(3): 199-211. (in Chinese)

[18] 李继国, 方淳. 基于SM9的指定验证者聚合签名方案[J]. 网络与信息安全学报, 2024, 10(4): 63-71.
Li Jiguo, Fang Chun. Designated verifier aggregate signature scheme based on SM9[J]. Chinese Journal of Network and Information Security, 2024, 10(4): 63-71. (in Chinese)

[19] 李继国, 朱留富, 刘成东, 等. 标准模型下证明安全的可追踪属性基净化签名方案[J]. 计算机研究与发展, 2021, 58(10): 2253-2264.
Li Jiguo, Zhu Liufu, Liu Chengdong, et al. Provably se-

cure traceable attribute-based sanitizable signature scheme in the standard model[J]. Journal of Computer Research and Development, 2021, 58(10): 2253-2264. (in Chinese)

[20] 唐飞, 凌国玮, 单进勇. 基于国产密码算法SM9的可追踪属性签名方案[J]. 电子与信息学报, 2022, 44(10): 3610-3617.
Tang Fei, Ling Guowei, Shan Jinyong. Traceable attribute signature scheme based on domestic cryptographic SM9 algorithm[J]. Journal of Electronics & Information Technology, 2022, 44(10): 3610-3617. (in Chinese)

[21] 朱留富, 李继国, 赖建昌, 等. 基于商密SM9的属性基在线/离线签名方案[J]. 计算机研究与发展, 2023, 60(2): 362-370.
Zhu Liufu, Li Jiguo, Lai Jianchang, et al. Attribute-based online/offline signature scheme based on SM9[J]. Journal of Computer Research and Development, 2023, 60(2): 362-370. (in Chinese)

[22] 周权, 陈民辉, 卫凯俊, 等. 基于SM9的支持策略隐藏的可追踪属性签名[J]. 计算机研究与发展, 2025, 62(4): 1065-1074.
Zhou Quan, Chen Minhui, Wei Kaijun, et al. Traceable attribute-based signature for SM9-based support policy hidden[J]. Journal of Computer Research and Development, 2025, 62(4): 1065-1074. (in Chinese)

[23] 董佶圣, 李聪, 沈子楠, 等. 面向区块链的UC安全门限SM9签名方案[J]. 计算机研究与发展, 2026, 63(1): 227-242.
Dong Jisheng, Li Cong, Shen Zinan, et al. Threshold SM9 signature scheme with UC security for blockchain[J]. Journal of Computer Research and Development, 2026, 63(1): 227-242. (in Chinese)

[24] 高睿, 丁昀, 高欣, 等. 基于国密SM9的密钥隔离签名[J/OL]. 软件学报, 2025: 1-11. https://doi.org/10.13328/j.cnki.jos.007469.
Gao Rui, Ding Yun, Gao Xin, et al. Key isolation signature based on state secret SM9[J/OL]. Journal of Software, 2025: 1-11. https://doi.org/10.13328/j.cnki.jos.007469.

[25] Cheng Z H. Security analysis of SM9 key agreement and encryption[C]//Information Security and Cryptology. Cham: Springer, 2019: 3-25.

[26] 赖建昌, 黄欣沂, 何德彪, 等. 国密SM9数字签名和密钥封装算法的安全性分析[J]. 中国科学(信息科学), 2021, 51(11): 1900-1913.
Lai Jianchang, Huang Xinyi, He Debiao, et al. Security analysis of SM9 digital signature and key encapsulation[J]. Science in China (Information Sciences), 2021, 51(11): 1900-1913. (in Chinese)

[27] 董佶圣, 李聪, 沈子楠, 等. 基于国密SM9的区块链匿名交易方案[J]. 中国科学: 信息科学, 2025, 55(6): 1428-1446.
Dong Jisheng, Li Cong, Shen Zinan, et al. An anonymous blockchain transaction scheme based on SM9[J]. Scientia Sinica (Informationis), 2025, 55(6): 1428-1446. (in Chinese)

[28] 赖建昌, 黄欣沂, 何德彪, 等. 基于商用密码SM9的高效分层标识加密[J]. 中国科学(信息科学), 2023, 53(5): 918-930.
Lai Jianchang, Huang Xinyi, He Debiao, et al. An efficient hierarchical identity-based encryption based on SM9[J]. Scientia Sinica (Informationis), 2023, 53(5): 918-930. (in Chinese)

[29] 李聪, 梁俊凯, 丁煜甲, 等. 基于SM9的分层标识广播内积函数加密[J]. 中国科学: 信息科学, 2024, 54(6): 1400-1418.
Li Cong, Liang Junkai, Ding Yujia, et al. Hierarchical identity-based broadcast inner product functional encryption based on SM9[J]. Scientia Sinica (Informationis), 2024, 54(6): 1400-1418. (in Chinese)

[30] Chuai Y, Zhang L Y, Xie S W, et al. Hierarchical identity-based encryption based on SM9[C]//Data Security and Privacy Protection. Singapore: Springer Nature, 2024: 106-118.

[31] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.

[32] 沈俊杰, 彭江, 郭坤银, 等. 车联网中基于位置信息映射和相关性评估的进化多任务优化算法[J]. 电子学报, 2025, 53(5): 1661-1676.
Shen Junjie, Peng Jiang, Guo Kunyin, et al. Location mapping and correlation assessment based evolutionary multi-task optimization algorithm in the Internet of vehicles[J]. Acta Electronica Sinica, 2025, 53(5): 1661-1676. (in Chinese)

[33] 许小龙, 杨威, 杨辰翊, 等. 车联网边缘计算环境下基于流量预测的高效任务卸载策略研究[J]. 电子学报, 2025, 53(2): 329-343.
Xu Xiaolong, Yang Wei, Yang Chenyi, et al. Efficient task offloading based on traffic prediction in IoV-enabled edge computing[J]. Acta Electronica Sinica, 2025, 53(2): 329-343. (in Chinese)

## 作者简介


**谢 佳** 女,1990年出生于河南省周口市。河南财经政法大学副教授。主要研究方向为公钥密码。

E-mail: xiejia199325@163.com

**王鲁玉** 女,1999年出生于河南省安阳市。河南财经政法大学硕士研究生。主要研究方向为格公钥密码。

E-mail: 2679947093@qq.com

**栾小杰** 男,2002年8月出生于河南省周口市。河南财经政法大学硕士研究生。主要研究方向为国密SM9算法。

E-mail: 891415794@qq.com

**高军涛** 男,1979年出生于河北省。西安电子科技大学副教授。主要研究方向为伪随机序列。

E-mail: jtgao@mail.xidian.edu.cn

**范长友** 女,2003年出生于河南省新乡市。河南财经政法大学硕士研究生。主要研究方向为环签名。

E-mail: 2174251324@qq.com

**王保仓** 男,1979年出生于河南省周口市。西安电子科技大学教授。主要研究方向为公钥密码。

E-mail: bcwang79@aliyun.com