基于IEEE、ETSI与YD/T 3957-2021标准的凭证管理系统比较

Abel C. H. Chen信息与通信安全实验室，中
华电信实验室ORCID：0000-0003-3628-3033

摘要——**随着车联网（车对万物）技术日益普及，车联网的安全在全球范围内受到越来越多的关注。在北美，主要采用IEEE 1609系列标准；欧洲采用ETSI系列标准；中国也制定了行业标准YD/T 3957-2021等。尽管这些标准存在一些共性，但也表现出差异。为实现这些标准之间的兼容性，分析其异同是一个关键问题。因此，本研究重点分析上述三大标准，讨论证书格式、已签名消息格式以及证书请求流程等方面。此外，本研究评估了不同密码学方法的效率，包括NIST P-256与SM2-256、SHA-256与SM3-256，以及AES-128与SM4-128。最后，本研究在V2X设备上实现了这三大标准，并比较了车联网中消息签名与签名验证的效率，为车联网安全证书管理系统的开发提供参考。**

关键词——***IEEE 1609.2.1***、***ETSI TS 102 941***、***YD/T 3957-2021***、***SM2***、***SM4***

I. 引言

近年来，为增强车联网的安全性，世界各地的组织开始根据各自的国情和环境，制定适用于本地区的车联网证书管理系统标准。在北美，主要标准包括 IEEE 1609.2 [1] 和 IEEE 1609.2.1 [2], , 以及安全凭证管理系统（SCMS）的设计 [3]-[4]。在欧洲，主要标准包括 ETSI TS 103 097 [5] 和 ETSI TS 102 941 [6], , 同时还开发了协作式智能交通系统（C-ITS）SCMS（CCMS）[7]-[8] 。与此同时，中国目前已制定 YD/T 3957-2021 [9], 等行业标准，并开发了中国安全凭证管理系统（C-SCMS）[10]。

尽管不同组织制定了各自的标准，但各方一直致力于确保这些标准之间的兼容性，以实现不同车联网设备之间的通信和身份认证。因此，近期国际标准逐渐采用更加统一的格式，同时允许根据各国的具体要求设置参数值。鉴于此，本研究重点分析三大主要标准之间的异同，探讨其优缺点，并对其性能进行评估和验证。本研究的贡献概述如下：

- 本研究比较了不同国家采用的车联网安全标准，包括 IEEE 1609 系列标准、ETSI 系列标准以及 YD/T 3957-2021 和相关标准。
- 本研究实现并比较了各种密码标准的计算效率。
- 本研究实现并比较了不同车联网安全标准的计算效率。

本文分为八个部分。第二节和第三节分析证书和签名消息的结构。第四节和第五节分析证书请求流程。第六节比较不同密码学方法的效率，第七节则比较不同标准在车联网设备上的效率。最后，第八节总结本研究的发现。

II. 证书的结构

为实现不同标准证书之间的兼容性，近年来，各种标准开始采用 IEEE 1609.2标准定义的 CertificateBase 格式（如图1所示）[1]。根据颁发者的不同，证书可分为两大类：注册证书和授权证书，具体如下。

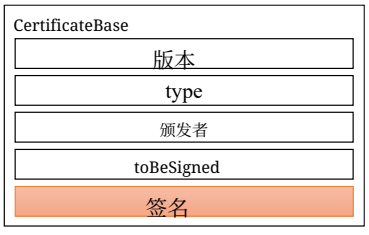

图1。 CertificateBase 的结构。

A. 注册证书 / 注册证书

在 SCMS 和 C-SCMS 中，每个车联网设备（称为终端实体（EE））都可以由注册证书颁发机构（ECA）颁发注册证书，该证书用作车联网设备的法定身份标识。同样，在 CCMS 中，每个车联网设备（称为 ITS站（ITS-S））都可以由注册机构（EA）颁发注册证书，作为其法定身份标识。注册证书和注册证书均基于 CertificateBase 格式。

B. 授权证书 / 授权票据

在 SCMS 和 C-SCMS 中，每个车联网设备都可以使用已颁发的注册证书向授权证书颁发机构（ACA）申请授权证书，以便在发送签名消息时使用。同样，在 CCMS 中，每个车联网设备都可以使用已颁发的注册证书向授权机构（AA）申请授权票据，以便在发送签名消息时使用。授权证书和授权票据均基于 CertificateBase 格式。

C. 注

值得注意的是，在类型字段中，SCMS 默认使用隐式证书，而 CCMS 和 C-SCMS 默认使用显式证书。此外，尽管 IEEE 1609.2 的 2022年 版本新增了对 SM2、SM3 和 SM4 的支持，但不同标准采用的密码学方法或参数仍略有差异，如表 I 所示。例如，在 SCMS 中，使用椭圆曲线数字签名算法（ECDSA）[11] 和 NIST P-256 进行签名；在 CCMS 中，使用 ECDSA 和 Brainpool P-256 进行签名；在 C-SCMS 中，则使用 SM2签名算法[12] 和 SM2-256 进行签名。

表 I.　默认密码学方法

密码学	SCMS	CCMS	C-SCMS
非对称密码学	NIST P-256	Brainpool P-256	SM2-256
Hash	SHA-256	SHA-256	SM3-256
对称密码学	AES-128	AES-128	SM4-128

III. 签名消息的结构

为了实现不同标准之间V2X数据包的兼容性，近年来各类标准已开始采用Ieee1609Dot2Data格式。其中，最常用的数据包是签名消息，主要定义于Ieee1609Dot2Data-Signed（如图2所示）[2]，以及签名加密消息，主要定义于Ieee1609Dot2Data-SignedEncrypted（如图3所示）[2]。

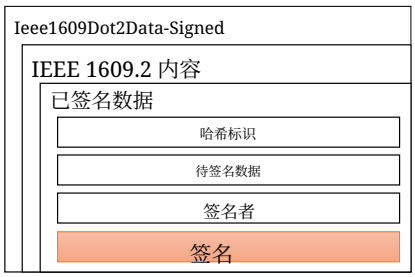

图2. Ieee1609Dot2Data-Signed的结构。



图3. Ieee1609Dot2Data-SignedEncrypted的结构。

A. *IEEE*的*SCMS*中的*Ieee1609Dot2Data-Signed*

在SCMS中，Ieee1609Dot2Data-Signed [2] 的结构如图2所示，主要包括四个字段：哈希标识、待签名数据、签名者和签名。以发送基本安全消息（基本安全消息）为例，设备将哈希标识设置为SHA-256，将待签名数据设置为ITS应用消息，将签名者设置为授权证书的哈希值，并使用椭圆曲线数字签名算法与NIST P-256生成签名，将所得签名置于签名字段中。

B. *ETSI*的*CCMS*中的*EtsiTs103097Data-Signed*

在 CCMS 中，EtsiTs103097Data-Signed [5] 的结构继承自 Ieee1609Dot2Data-Signed，其字段信息与图 2 所示相同。值得注意的是，ETSI 分别定义了合作感知消息（CAM）和分布式环境通知消息（DENM），二者均继承自 EtsiTs103097Data-Signed，因此仍遵循 Ieee1609Dot2Data-Signed格式。以发送 CAM 为例，ITS-S 将哈希标识设置为 SHA-256，将待签名数据设置为 ITS应用消息，将签名者设置为授权票据的哈希值，并使用基于 Brainpool P-256 的椭圆曲线数字签名算法生成签名，将生成的签名置于签名字段中。

C. *C-SCMS* 中的 *V2XSecData-Signed*

在 C-SCMS 中，V2XSecData-Signed [9] 的结构继承自 Ieee1609Dot2Data-Signed，其字段信息与图 2 所示相同，主要包括哈希标识、待签名数据、签名者和签名四个字段。在命名方面，将“Ieee1609Dot2”替换为“V2XSec”，并将提供商服务标识符（PSID）更改为应用标识符（AID），而大多数其他结构均继承自 IEEE标准。以发送基本安全消息（BSM）为例，设备将哈希标识设置为 SHA-256，将待签名数据设置为 ITS应用消息，将签名者设置为授权证书的哈希值，并使用 SM2签名算法和 SM2-256 生成签名，将生成的
签名字段中的签名。

IV. 注册证书请求比较

A. *IEEE* 的 *SCMS* 中的注册证书请求

在 SCMS 中，该流程始于设备向 ECA 发送 EeEcaCertRequestSpdu，并使用预置规范私钥对请求进行签名，同时在请求中包含注册公钥。EeEcaCertRequestSpdu 是一种签名证书请求。ECA 使用预置规范公钥验证请求的签名和内容后，向设备发送 EcaEeCertResponseSpdu，其中包含设备的注册证书。ECA 对此响应进行签名，EcaEeCertResponseSpdu 是 Ieee1609Dot2Data-Signed 的一种形式，如图 4 所示。

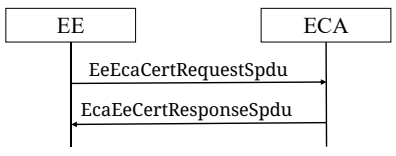

图 4. IEEE 的 SCMS 中的注册证书请求。

B. ETSI CCMS 中的注册证书请求*'s CCMS*

在 CCMS 中，该流程始于设备向注册机构发送 EnrolmentRequest，并同时使用预置规范私钥和注册私钥对请求进行签名。请求中包含注册公钥，并使用注册机构的公钥加密。EnrolmentRequest 是 Ieee1609Dot2Data-SignedEncrypted 的一种类型。注册机构使用预置规范公钥以及请求中的注册公钥验证请求的签名和内容后，向设备发送 EnrolmentResponse。EnrolmentResponse 包含设备的注册证书，并由注册机构进行签名和加密。EnrolmentResponse 是 Ieee 1609Dot2Data- SignedEncrypted 的一种形式，如图 5 所示。

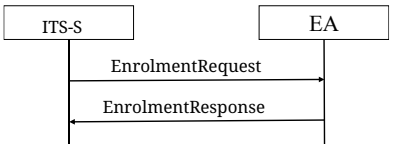

图 5. ETSI CCMS 中的注册证书请求。

C. C-SCMS 中的注册证书请求

在 C-SCMS 中，可通过设备配置管理器（DCM）机制和通用引导架构（GBA）机制建立安全连接并发送证书请求。以 3GPP [13] 定义的 GBA机制为例，设备与 GBA认证系统（AS）建立安全连接，随后通过此安全连接发送 EeEcaCertRequestSpdu 并接收 EcaEeCertResponseSpdu，如图 6 所示。EeEcaCertRequestSpdu 和 EcaEeCertResponseSpdu 与第 IV.A 小节中的描述一致。

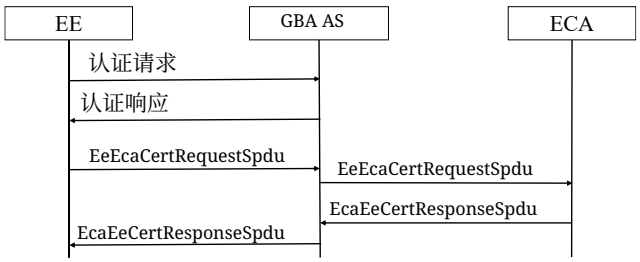

图 6. C-SCMS 中的注册证书请求。

V. 授权证书请求的比较

A. IEEE 的 *SCMS* 中的授权证书请求

在 SCMS 中，设备（EE）获得注册证书后，可以向注册机构（RA）发送 EeRaCertRequestSpdu，并使用注册私钥对请求进行签名。该请求包含设备的注册证书和毛毛虫公钥，随后使用 RA 的公钥加密。EeRaCertRequestSpdu 是一种签名加密消息。RA 从注册证书中提取设备的注册公钥，以验证请求的签名和内容。验证成功后，RA 向设备发送 RaEeCertAckSpdu。此外，RA 根据毛毛虫公钥生成茧公钥，并向 ACA 发送 RaAcaCertRequestSpdu；该请求包含茧公钥，并使用 RA的私钥进行签名。RaAcaCertRequestSpdu 是一种签名消息。ACA 验证签名和请求内容后，会向 RA 发送 AcaRaCertResponseSpdu。AcaRaCertResponseSpdu 包含 Aca响应，其中包括设备的授权证书，以及包含蝴蝶公钥的授权证书（或隐式证书的重构值）。最后，设备向 RA 发送 EeRa下载请求 SPDU，请求下载授权证书。RA 向设备提供一个包含 RaEe证书信息和 Aca响应 的 ZIP文件，如图 7 所示。EeRa下载请求SPDU 是一种 Ieee1609Dot2Data-SignedEncrypted。值得注意的是，在 SCMS 中，RA 负责验证设备注册证书的合法性。

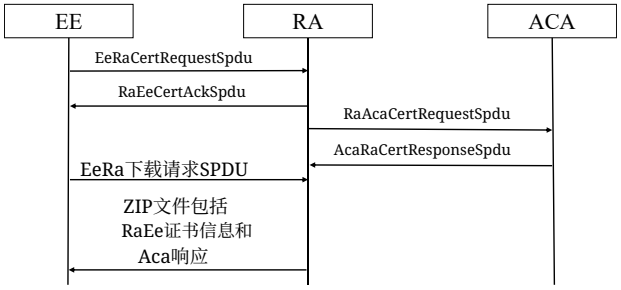

图 7。 IEEE 的 SCMS 中的授权证书请求 SCMS。

B. ETSI 的 *CCMS* 中的授权票证请求

在 CCMS 中，ITS-S 获取注册证书后，可以向授权机构发送 AuthorizationRequest，并使用授权私钥对请求进行签名。该请求包括授权公钥和 EcSignature，其中 EcSignature 由设备使用注册证书和注册私钥进行签名。随后，使用授权机构的公钥对请求进行加密。AuthorizationRequest 属于签名加密消息。需要注意的是，在此阶段，授权机构仅使用授权公钥验证请求的签名，而不会验证 ITS-S 注册证书的合法性。EcSignature 被封装在 AuthorizationValidationRequest 中，该请求由授权机构签名

使用其私钥，并使用注册机构的公钥加密后发送给注册机构。当注册机构收到授权验证请求时，它会同时验证授权验证请求的签名和EcSignature的签名，并确认相关信息。验证成功后，注册机构向授权机构回复授权验证响应。授权验证请求和授权验证响应都属于签名加密消息。最后，授权机构签发智能交通系统站的授权票据，并将其封装在授权响应中发回智能交通系统站，如图8所示。值得一提的是，CCMS中没有RA角色，CCMS中的注册机构承担了SCMS中RA的部分功能，例如验证智能交通系统站注册证书的合法性。

C. C-SCMS 中的授权证书请求

在 C-SCMS 中，DCM机制和GBA机制也可用于建立安全连接并申请授权证书请求。以 3GPP [13] 定义的 GBA机制为例，设备通过

认证请求和认证响应。在建立此安全连接后，设备会发送 EeRaCertRequestSpdu 并接收 RaEeCertAckSpdu，如图 9 所示。涉及 EeRaCertRequestSpdu、RaEeCertAckSpdu 及后续步骤的流程与 V.A 小节所述一致。值得注意的是，在 C-SCMS 中，RA 称为假名注册机构（PRA）。

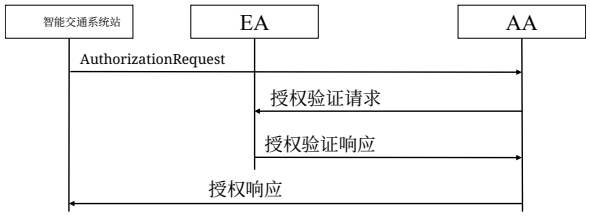

图8. ETSI 的 CCMS 中的授权票证请求 .

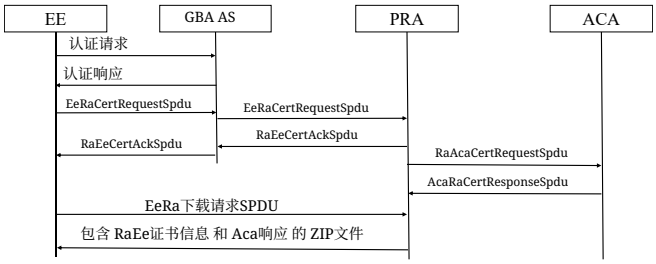

图9. C-SCMS 中的授权证书请求。

VI. 密码学方法的性能比较

为评估不同密码学方法的计算效率，本节在一台笔记本电脑上实现了表 I 中列出的方法。硬件和软件配置包括 Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz、16.0 GB RAM、Windows 10企业版、Java 18.0.2.1 和 BouncyCastle 1.78。以下各小节将分别评估椭圆曲线密码（ECC）数字签名、ECC加密与解密、哈希算法以及对称加密与解密的性能。

A. 用于签名的 *NIST P-256* 和 *SM2-256*

本小节评估椭圆曲线数字签名算法和 SM2签名算法的计算效率。椭圆曲线数字签名算法 [11] 采用椭圆曲线 NIST P-256，SM2签名算法 [12] 采用椭圆曲线 SM2-256。每种算法均执行 3000 次，以测量密钥生成时间、签名生成时间和签名验证时间。实验结果如图10所示。

从结果可以看出，椭圆曲线数字签名算法和 SM2签名算法的密钥生成过程相似：两者都需要随机生成一个整数，然后根据该值计算一个椭圆曲线点，因此计算时间没有显著差异。然而，在签名生成过程中，SM2 需要额外进行一次哈希计算，因此签名创建耗时更长。最后，对于签名
验证方面，椭圆曲线数字签名算法与SM2签名算法之间没有显著差异。

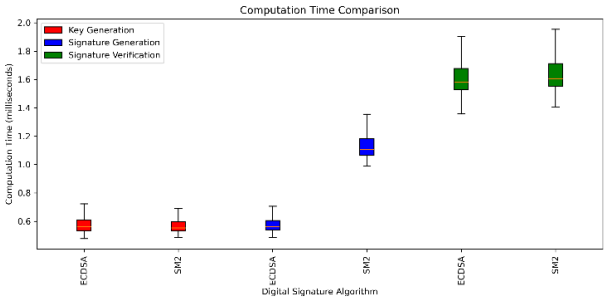

图 10. NIST P-256 与 SM2-256 的签名比较。

B. NIST P-256 与 *SM2-256* 加密

本小节评估了常用于加密和解密的ECIES（椭圆曲线集成加密方案）的计算效率。该方案主要用于封装或协商共享对称密钥。测试的算法包括基于椭圆曲线NIST P-256 [14] 的ECIES和基于椭圆曲线SM2-256 [15], 的ECIES，每种算法均执行3,000次，以测量密钥生成时间、密钥封装时间和密钥提取时间。实验结果如图11所示。

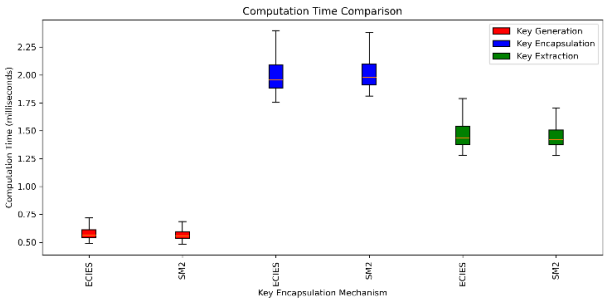

图 11. NIST P-256 与 SM2-256 加密对比。

结果表明，在使用相同 ECIES 算法的情况下，无论采用 NIST P-256 椭圆曲线还是 SM2-256 椭圆曲线，密钥生成时间、密钥封装时间和密钥提取时间均无显著差异。

C. SHA-256 与 *SM3-256*

本小节评估不同哈希算法的计算效率，具体来说，实现并测试了 SHA-256 [16] 和 SM3-256 [15]。实验中执行了 3,000 次哈希运算，以测量哈希计算时间。实验结果如图 12 所示。

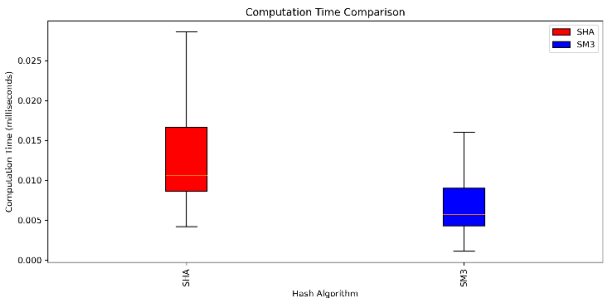

图 12. SHA-256 与 SM3-256 对比。

从结果可以看出，SM3-256 的计算效率更高，计算时间显著更短

与 SHA-256 相比。因此，未来可考虑采用 SM3-256 来提高计算效率。

D. AES-128和SM4-128

本小节通过实现并测试AES-128 [17] 和SM4-128 [18]，评估不同对称加密与解密算法的计算效率。实验中，每种算法均执行3,000次，以测量加密和解密的计算时间。实验结果如图13所示。

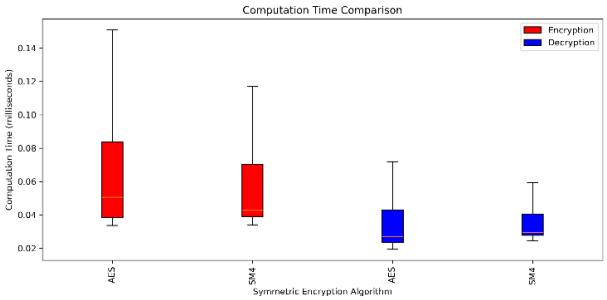

图13. AES-128和SM4-128的比较。

从结果可以看出，与AES-128相比，SM4-128的加密和解密计算时间均略短。因此，尽管SM4-128的计算效率较高，但差异在统计学上并不显著，这表明AES-128和SM4-128的计算效率相近。

VII. 在车联网设备中的实现

为验证SCMS、CCMS和C-SCMS标准在车联网设备上的执行性能，本节将使用可信电子设备对其进行实现和测试。第VII.A小节介绍实验环境，第VII.B小节展示计算时间的对比实验结果。

A. 实验环境

在本研究的实验环境中，使用 Clientron 的车载单元（车载单元）作为 V2X设备，以实现 SCMS、CCMS 和 C-SCMS 标准。V2X设备的硬件和软件规格包括 MT2712芯片、Android 10 和 BouncyCastle 1.78。每台 V2X设备申请注册证书和授权证书/授权票据后，都会按照 IEEE . . . 中定义的 Ieee 1609 2 Dot [2] 14 Data-Signed 格式发送和接收基本安全消息。实现界面如图 . 所示。

B. 计算时间比较

发送基本安全消息时，V2X设备需要将其封装为Ieee1609Dot2Data-Signed 格式，并为该消息生成签名，以证明发送方的合法性。授权证书/授权票据被置于签名者字段中，以便接收方进行验证。图15展示了在SCMS、CCMS和C-SCMS标准下，生成包含BSM信息的Ieee1609Dot2Data-签名消息所需的计算时间。可以看出，尽管SCMS和CCMS分别采用不同的椭圆曲线NIST P-256和Brainpool P-256，但由于二者均使用椭圆曲线数字签名算法，计算时间并无显著差异。然而，C-SCMS使用SM2签名算法，如第VI.A小节所述，该算法需要更多计算时间。因此，C-SCMS实现生成包含BSM信息的数据包所需的时间更长。

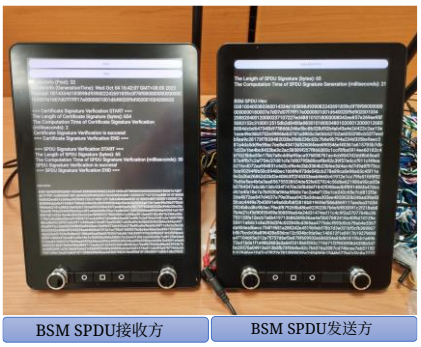

图 14. 基于 Clientron 车载单元的车联网设备实现。

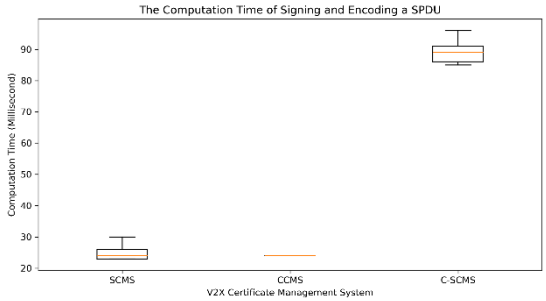

图 15. 签名生成的计算时间比较。

在验证包含基本安全消息的数据包时，接收方 V2X设备需要从数据包中获取授权证书/授权票据。随后，它使用授权证书/授权票据获取发送方 V2X设备的公钥，以验证数据包。图 16 展示了在 SCMS、CCMS 和 C-SCMS 标准下，验证包含基本安全消息信息的 Ieee1609Dot2Data签名消息所需的计算时间。可以看出，CCMS 和 C-SCMS 默认使用显式证书，因此证书中包含发送方 V2X设备的实际公钥。这使得系统能够直接使用公钥验证签名，从而缩短计算时间。相比之下，SCMS 默认使用隐式证书，其中仅包含重构值。因此，需要使用 ACA公钥重构发送方 V2X设备的实际公钥，导致计算时间更长。

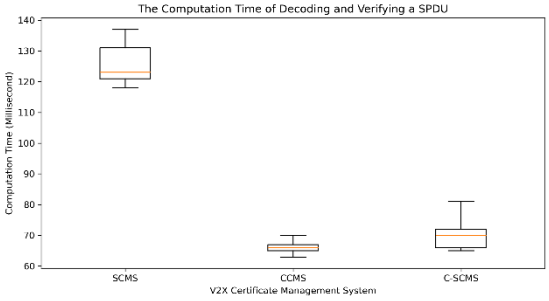

图 16. 签名验证的计算时间比较。

VIII. 结论与未来工作

本研究主要探讨 SCMS、CCMS 和 C-SCMS 三项标准，基于消息流和密码学方法方面的差异对其进行比较与验证，并从原理到实现展开全面讨论和验证。

研究结果表明，国际标准正逐步趋于兼容。证书格式现已完全兼容，签名消息数据包格式也可实现一致。主要差异在于证书申请流程以及用于证书请求的数据包，还有密码学方法及其参数。此外，本研究发现，椭圆曲线数字签名算法在签名效率上优于SM2，而SM3在哈希计算效率上的表现优于SHA。另外，CCMS和C-SCMS默认使用显式证书，因此在验证安全数据包方面的效率高于SCMS。

尽管本研究发现SCMS在验证安全数据包方面效率较低，但这可能是不公平的比较。未来工作可在CCMS和C-SCMS中实现隐式证书，从而基于隐式证书对这三项标准进行比较。

致谢

本研究开发的RCA证书已在OmniAir互操作性测试会成功通过互操作性测试，并由SCMS管理器正式列入测试证书信任列表（CTL），详见：https://www.scmsmanager.org/publications/。此外，该证书也已获得认可并被纳入由欧盟C-ITS联络点（CPOC）维护的欧洲证书信任列表（ECTL），访问地址为：https://cpoc.jrc.ec.europa.eu/ECTL.html。我们衷心感谢OmniAir、SCMS管理器、CPOC及所有其他合作伙伴在整个过程中给予的关键支持与贡献。

参考文献

[1] “车载环境无线接入——应用和管理消息的安全服务 IEEE 批准草案标准”，载于*IEEE 1609.2-2022*标准（修订 *IEEE Std 1609.2- 2016*），第 1-349 页，2023年3月，doi：10.1109/IEEESTD.2023.10075082。[2] “车载环境无线接入（WAVE）标准——终端实体的证书管理接口”，载于*IEEE 1609.2.1-2022*标准（修订 *IEEE Std 1609.2.1-2020*），第 1-261 页，2022年6月，doi：10.1109/IEEESTD.2022.9810154。[3] B. Brecht 等，“面向车联网通信的安全凭证管理系统”，载于*IEEE*智能交通系统汇刊，第 19 卷，第 12 期，第 3850-3871 页，2018年12月，doi：10.1109/TITS.2018.2797529。[4] A. C. H. Chen、B. -Y. Lin、C. -K. Liu 和 C. -F. Lin，“基于 IEEE 1609.2 和 1609.2.1 标准的安全凭证管理系统实现与性能分析”，载于*2023*年*IEEE*机器学习与应用网络国际会议（*ICMLANT*），萨尔瓦多圣萨尔瓦多，2023年，第 1-5 页，doi：10.1109/ICMLANT59547.2023.10372990。[5] “智能交通系统（ITS）；安全；安全报头和证书格式；第 2 版”，载于*ETSI TS 103 097 V2.1.1*，第 1-22 页，2021年10月。[6] “智能交通系统（ITS）；安全；信任与隐私管理；第 2 版”，载于*ETSI TS 102 941 V2.2.1*，第 1-94 页，2022年11月。[7] Y. Gong 和 B. -J. Hu，“在 C-V2X 中利用区块链的抗量子密钥管理方案”，载于*IEEE*智能交通系统汇刊，提前在线发表，doi：10.1109/TITS.2024.3421381。[8] A. C. H. Chen、B. -Y. Lin、C. -K. Liu 和 C. -F. Lin，“基于 IEEE 1609.2.1 和 ETSI TS 102 941 的 V2X凭证管理系统比较”，2024年 IEEE 北卡纳塔克邦分会旗舰国际会议（NKCon），印度贝拉加维，2023年，第 1-6 页。[9] “基于 LTE 的车载通信——安全证书管理系统技术要求”，载于工业和信息化部公告，*YD/T 3957-2021*，第 1-173 页，2021年12月。[10] X. Wu、H. Ning、S. Sun、K. Qian、J. Fang、X. Wang 和 B. Wang，“车联网电子认证服务管理建议”，载于信息通信技术与政策，第 50 卷，第 3 期，第 60-65 页，2024年3月，doi：10.12267/j.issn.2096-5931.2024.03.009。[11] X. Yang、M. Liu、M. H. Au、X. Luo 和 Q. Ye，“高效的可验证加密类 ECDSA 签名及其应用”，载于*IEEE*信息取证与安全汇刊，第 17 卷，第 1573-1582 页，2022年，doi：10.1109/TIFS.2022.3165978。[12] Y. Zhang 等，“基于 SM2数字签名算法的可验证随机函数方案及其在委员会选举中的应用”，载于*IEEE*计算机学会开放期刊，第 5 卷，第 480-490 页，2024年，doi：10.1109/OJCS.2024.3463649。[13] “第三代合作伙伴计划；技术规范组服务和系统方面；通用认证架构（GAA）；通用引导架构（GBA）（第 18 版）”，载于*3GPP TS 33.220 V18.3.0*，第 1-110 页，2024 年 3 月。[14] P. Realpe-Muñoz 、 J. Velasco-Medina 和 G. Adolfo-David，“采用 GF(2m) 上高斯正规基设计 S-ECIES 密码处理器”，载于*IEEE*超大规模集成电路（*VLSI*）系统汇刊，第 29 卷，第 4 期，第 657-666 页，2021年4月，doi：10.1109/TVLSI.2021.3057985。[15] X. Zheng、C. Xu、X. Hu、Y. Zhang 和 X. Xiong，“SM2/3/4 加解密与数字签名系统的软硬件协同设计与实现”，载于*IEEE*集成电路与系统计算机辅助设计汇刊，第 39 卷，第 10 期，第 2055-2066 页，2020年10月，doi：10.1109/TCAD.2019.2939330。[16] A. C. H. Chen，“哈希算法性能报告——案例研究：基于区块链系统的加密货币交易所”，载于*2024*年*IEEE*数据智能与认知信息学国际会议（*ICDICI*），印度蒂鲁内尔维利，2024年，第 1-6 页。[17] W. -K. Lee、H. J. Seo、S. C. Seo 和 S. O. Hwang，“在图形处理器上高效实现 AES-CTR 和 AES-ECB，并应用于高速 FrodoKEM 和穷举密钥搜索”，载于*IEEE*电路与系统*II*汇刊：简报，第 69 卷，第 6 期，第 2962-2966 页，2022年6月，doi：10.1109/TCSII.2022.3164089。[18] W. Liu 等，“具有双重 DPA攻击对策的 128 Gbps 流水线SM4电路”，载于*IEEE*超大规模集成电路（*VLSI*）系统汇刊，第 32 卷，第 6 期，第 1164-1168 页，2024年6月，doi：10.1109/TVLSI.2024.3379205。