基于隐式证书的嵌入式设备证书压缩方法

米轩浩[1] 王中华[1] 吴雨婷[1]
MI Xuanhao WANG Zhonghua WU Yuting

摘 要 嵌入式设备之间的身份认证是建立安全通信链接的基础，也将直接影响嵌入式设备及网络的攻击面暴露风险与攻击方式数量。传统的公钥基础设施（PKI）显式证书方法虽然可以解决身份认证问题，但高度依赖于设备的网络计算资源且效率较低。针对上述问题，提出了一种基于隐式证书的嵌入式设备证书压缩方法。首先采用标准 MES（minimal ASN.1 encoding scheme）方案生成 DER 编码的隐式证书作为嵌入式设备身份认证基础，并引入 CBOR（concise binary object representation）编码对 MES 隐式证书进行压缩与优化，同时由于 CoAP（constrained application protocol）协议支持 CBOR 编码证书的自动解析，二者配合可以有效提升嵌入式设备之间的身份认证效率。实验结果表明，相较于传统显式证书、DER 编码隐式证书和 PEM 编码隐式证书，基于 CBOR 编码压缩的隐式证书大小分别减少了 75.3%、20.6% 与 40.6%，解决了设备身份认证过程中计算资源耗费过多的问题，为资源受限的嵌入式设备网络的安全通信提供了有效保证。

关键词 嵌入式设备；公钥基础设施（PKI）；隐式证书；DER 编码；PEM 编码；简明二进制对象表示（CBOR）；CoAP 协议

doi：10.3969/j.issn.1672-9528.2024.03.016

0 引言

近年来，嵌入式设备通信技术的迅速发展，已经深深渗透到了我们的日常生活和工作中，无论是智能家电、医疗设备还是工业控制系统，都通过嵌入式设备通信技术相互链接，实现了设备之间数据的快速传输和处理。嵌入式设备通信技术的发展不仅为各类设备带来了数据传输与数据处理能力的极大提升，还促进了各行业应用的深化和扩展，然而这一过程也暴露出一系列的安全问题。

由于嵌入式设备的计算能力与存储空间有限，它们在面对复杂的安全威胁时往往显得力不从心。如果通信设备双方在建立通信连接之前不对双方进行安全的身份认证，那么恶意攻击者可能会利用这一弱点，对设备进行非法入侵、数据篡改或远程控制，从而对个人隐私和整个系统的安全构成严重威胁。

针对这一问题，学者们进行了广泛而深入的研究。他们提出了一系列算法和技术手段，以提高嵌入式设备的安全性能和防范能力。这些算法和技术包括加密算法、防火墙技术、入侵检测技术等。在嵌入式设备通信的身份认证方面，很多学者已经取得了一些重要的研究成果。其中与隐式证书相关的有 Brown 与 Pinstov 等人提出的 OMC[1]、基于 MC 的 ECQV[2]、Paulo 等人设计的基于 Schnorr 签名与 OMC 的算法 [3]、Min Zhao 等人提出的基于自签名隐式证书的认证密钥协商协议研究 [4] 以及 Kaixuan Wang 等人提出的隐式证书的国密算法应用研究 [5]。

本文基于 ECQV 隐式证书与 CBOR 编码，提出了一种适合嵌入式设备特殊场景需求（带宽、算力、存储空间等受限）的证书压缩方法。本文将比较通用显式证书、标准 DER 编码的隐式证书、PEM 编码的隐式证书以及使用 CBOR 编码压缩的隐式证书的证书大小。同时，使用 CBOR 隐式证书结合 CoAP 协议，确保嵌入式设备在建立通信连接之前进行设备间安全的身份认证，防止恶意攻击者利用此弱点对系统进行网络攻击。

1 公钥基础设施介绍

公钥基础设施（PKI）[6] 是保障网络安全的重要手段之一，它基于公钥密码学提供身份认证、数据加密和数字签名等服务。在电子商务、电子政务和金融等领域，PKI 得到了广泛的应用。

PKI 的核心组成部分包括认证中心（CA）、证书注册机构（RA）和证书库等。其中，认证中心负责签发和管理数字

1. 航空工业西安航空计算技术研究所 陕西西安 710065

证书，提供身份验证服务；证书注册机构负责对用户进行身份验证，并注册数字证书；证书库则用于存储和管理数字证书。这些组件相互协作，共同保障网络通信的安全性。

相对于其他身份认证技术，PKI 具有更高的可靠性和安全性，它采用公钥密码学算法，对数据进行加密和解密，确保数据的机密性和完整性。同时，PKI 还提供了数字签名功能，用于验证信息的真实性和完整性。然而 PKI 也存在一些局限性，如证书管理复杂、证书吊销和更新等问题，尤其是嵌入式设备中如果使用标准的 X.509 显式证书虽然能解决身份认证问题，但对于资源受限的嵌入式设备网络来说，这个证书认证方法效率较低且耗费过多资源。因此，需要寻找一种轻量级的证书身份认证方法解决这个问题。

2 隐式证书

2.1 隐式证书简介

隐式证书是一种公钥证书，是一种通用目的 PKI 证书方案。相比于传统的 X.509 显式证书，隐式证书特别适合资源受限场景（带宽、算力、存储空间等），为用户提供数字身份凭证。

X.509 显式证书包含多个部分，包括证书颁发机构信息、证书持有人信息、公钥以及签名，其中签名是最重要的部分，用于验证证书是否真实有效。在验证证书时，浏览器会使用相应的公钥对证书进行解密并检查签名是否真实有效，若签名错误或证书已过期，则不会建立安全连接。此外，X.509 证书还附带了证书吊销列表和用于对证书进行签名的证书签发机构直到最终可信点为止的证书合法性验证算法。

由于显式证书的认证方法效率较复杂且耗费过多资源，而隐式证书中不直接包含 CA 的数字签名与公钥，在使用隐式证书时需要利用隐式证书的密钥进行运算来完成对证书的合法性验证。相较于显式证书而言，隐式证书所需资源更少，更适合嵌入式环境下的身份认证过程。

2.2 隐式证书具体格式介绍

ECQV 方案提出了 3 种可能的隐式证书编解码方案。

（1）Fixed-Length Fields 方案：固定长度、固定字段、内容可自定义的 ASN.1 语法描述方式。

（2）MES（minimal ASN.1 encoding scheme）方案：一种 ASN.1 的 DER 编码机制，使用简洁、固定长度字段、可移植性高的编码方案。

（3）X.509 兼容方案：证书可以被解析成 X.509 格式。该方案的证书格式的定义和规范与显式证书相同。

本文将采用 ECQV 标准 [7] 中 DER 编码的 MES 证书，为基础对隐式证书进行进一步的压缩与优化。证书包含的具体字段与格式如图 1 所示。

```
ANSI-X9-YY{iso(1) member-body(2) us(840) 10045 module(0) 2}

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

ansi-X9-YY OBJECT-IDENTIFIER ::= {iso(1) member-body(2) us(840) 10045}

ECQVCertificate  ::=  SEQUENCE  {
    type MESType DEFAULT t1,-- one byte, see below
    serialNumber    OCTET STRING (SIZE (8)),
    curve Curve,-- named curve, see below
    hash Hash,
    issuerID  OCTET STRING (SIZE (8)),
    validFrom   OCTET STRING (SIZE (5)),-- 40-bit Unix time
    validDuration   OCTET STRING (SIZE (4)),-- 32-bit # of seconds
    subjectID  OCTET STRING (SIZE (8)),
    usage KeyUsage,  -- one byte, described below
    pubKey OCTET STRING,
    pathLenConstraint INTEGER (0..255) OPTIONAL,
    ...,
    -- Extensions:
    algorithm[1]    AlgorithmIdentifier OPTIONAL,
    email[2] IA5String (SIZE (0..128)) OPTIONAL
}
```

图 1 标准 MES 方案证书包含字段与格式

MES 方案隐式证书具体包含下列具体字段。

Type：这个字段代表证书类型，其中 0 代表没有扩展字段，1 代表有扩展字段。

SerialNumber：此字段代表证书的序列号，即从 CA 分配的唯一编号，即使两个证书由同一 CA 颁发，也不可能具有相同的序列号。因此，需要一个大小为 8 Byte 的八位字节字符串作为唯一的序列号。

Curve：ECQV 证书生成时使用的 ECC 椭圆曲线名称。

Hash：用于 ECQV 证书生成时使用的加密哈希函数名。

IssuerID：这是证书颁发者 CA 的 8 Byte 标识符。

ValidFrom：此 5 Byte 字段表示证书在 Unix 时间内的有效性，表示为自 1970 年 1 月 1 日以来经过的秒数。

ValidDuration：一个 4 Byte 的字段，表示证书有效性的结束时间（以秒为单位），从字段 ValidFrom 开始生效。

SubjectID：一个唯一的 8 Byte 标识符，用于标识相对于此证书中公钥的私钥所有者。

Usage：此字段根据 RFC 5280 定义了证书中包含的密钥的有效用途。

pubKey：由 ECQV 算法计算的值。此字段允许重建公钥并同时隐式验证证书（在使用公钥验证签名时），大小取决于所选 ECC 曲线的类型。如果使用 secp256r1 曲线，此公钥就为 33 Byte。由于数据块长度不定，使用 DER 编码后此字段长度为 37 Byte（类型标志 1 Byte+ 数据块长度 0x80 表示长度不定 1 Byte+ 公钥长度 1 Byte+2 Byte 数据块结束标志）。

2.3 基于 PEM 编码的隐式证书

PEM（privacy enhanced mail）编码证书是一种基于 Base64 编码的密钥证书格式 [8]，它使用标准的 ASCII 码表示二进制数据，这种证书格式被广泛应用于在网络上进行传输和存储证书。

PEM 编码证书具有可读性高、通用性强、易于转换以及安全可靠的优点，人们可以直接在文本编辑器中查看和编辑 PEM 编码的证书，且 PEM 编码证书是一个标准的证书格式，

许多工具和软件都支持 PEM 证书的读取写入和处理，这使得它在证书管理、安全通信等方面具有很高的实用性。PEM 编码证书可以很容易地转换为其他格式的证书，例如 DER 格式、PKCS#7 格式等，这使得它在证书迁移备份和恢复方面有很高的灵活性。

然而，PEM 编码证书是基于 Base64 编码的密钥证书格式，Base64 编码的转换规则是将每 3 Byte 的数据转换为 4 Byte 的 Base64 字符。本文中标准的隐式证书（DER 编码证书）转换为 PEM 证书后，证书的大小由 92 Byte 增加为 123 Byte。

3 基于 CBOR 编码的隐式证书压缩方法

CBOR（concise binary object representation）[9] 是一种新型的数据交换格式，它提供了一种高效、紧凑的方式来表示和交换结构化数据。CBOR 符合 RFC7049 中的 IETF 标准，它与传统的 ASN.1 是两种不同的二进制数据表示和交换格式。

ASN.1（abstract syntax notation one）[10] 是一种更早的二进制序列化方式，它使用一种基于规范的语法来描述数据结构。ASN.1 具有一种内建的类型系统，可以描述复杂的数据结构，并且支持多种编码模式，如 BER（basic encoding rules）和 PER（packed encoding rules）。这种灵活性使它可以描述复杂的数据结构，并且能够支持跨平台、跨语言的数据交换。然而，ASN.1 的缺点在于其相对较高的复杂性和冗长的编码。ASN.1 需要遵循严格的语法规范，因此在使用它进行数据序列化时需要编写大量的规范定义。此外，ASN.1 的解码速度可能比 CBOR 慢，因此在一些高性能场景中不是最佳选择。

相比之下，CBOR 是一种相对较新的数据交换格式，旨在提供良好的压缩性、扩展性且不需要进行版本协商。它使用二进制编码，相对于文本格式更加紧凑，减少了存储和传输的数据量。因此，本文尝试使用 CBOR 编码压缩 ASN.1 编码的隐式证书，缩小证书大小，提高嵌入式设备之间身份认证的效率。

针对上一节中 ECQV 算法生成的标准 ASN.1 编码证书的各个字段，本文分别作出以下处理。

Type：默认证书不需要拓展字段，即可删除此字段，即处理时默认此字段值为 0，可压缩 3 Byte。

SerialNum：该字段是必不可少的，因此仅可通过 CBOR 编码来进行压缩。与 ASN.1 编码相比，CBOR 编码的开销减少 1 Byte，字段的总大小从 10 Byte 减少到 9 Byte。图 2 和图 3 详细显示了通过 CBOR 编码实现的序列号字段大小的压缩。

```
0x04    //Octet String
0x08    //Size 8
0x01 0x23 0x45 0x67 0x89 0xab 0xcd 0xef
//此字段值为 01-23-45-67-89-ab-cd-ef
```

图 2 SerialNum 字段使用 ASN.1 编码（10 Byte）

```
0x48    //Byte Array,  Size 8
0x01 0x23 0x45 0x67 0x89 0xab 0xcd 0xef
//此字段值为 0x0123456789abcdef
```

图 3 SerialNum 字段使用 CBOR 编码压缩（9 Byte）

Curve：约定此证书使用 secp256r1 椭圆曲线 [11]，即可省去此字段，压缩 3 Byte。

Hash：约定此证书使用国密 SM3[12] 哈希算法，即可省去此字段，压缩 3 Byte。

IssuerID：ASN.1 编码中的 10 Byte 八位字节字符串通过 CBOR 编码压缩为 9 Byte。对于自签名证书，此值设置为 0。

Validfrom+ValidDuration：使用 CBOR 编码为 CBOR 中的字节串，将大小从 13 Byte 减少到 11 Byte。

SubjectID：同样的 CBOR 编码可将大小从 10 Byte 减少到 9 Byte。

Usage：由于证书用途固定，此字段也可被删除省略，压缩证书 3 Byte。

PubKEY：由 ECQV 算法计算的值。此字段允许重建公钥并同时隐式验证证书（在使用公钥验证签名时）。这取决于所选曲线的类型，secp256r1 的此字段的 CBOR 编码大小为 35 Byte（由于公钥长度为 33 Byte 大于 24 Byte，因此需要 2 Byte 表示字符串数据类型以及字符串长度）。相较于 ASN.1 编码的证书压缩 2 Byte。

压缩前 ASN.1 编码隐式证书大小为 92 Byte，压缩后的 CBOR 编码隐式证书大小为 73 Byte，压缩率为 21%，使用 CBOR 编码极大地缩小了 ECQV 隐式证书的大小，提高了嵌入式设备之间身份认证的效率。具体各字段压缩前后的编码所占字节数对比图如图 4 所示。使用 secp256r1 椭圆曲线的显式证书，DER 编码隐式证书，PEM 编码隐式证书以及 CBOR 编码隐式证书大小比较如图 5 所示。

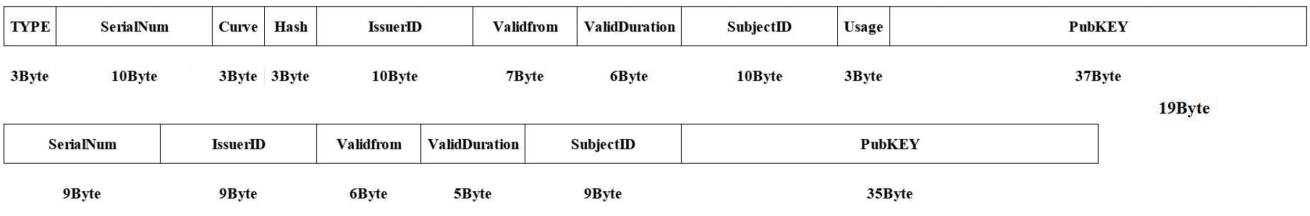

图 4 证书压缩前后字段编码大小对比图

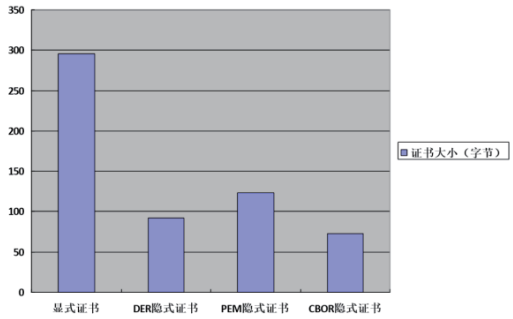

图 5 各类证书大小对比

由于显式证书大小取决于多种因素，包括但不限于证书的版本、包含的扩展、签名算法、证书的主题、颁发者信息以及附加的证书链等，一般使用 secp256r1 椭圆曲线的 X509 显式证书（DER 编码）大小由 296 ～ 2000 Byte 不等，本图中采用最小的显式证书进行其大小的比较。

CoAP（constrained application protocol）协议是一种应用于物联网网络的轻量级协议，它的详细规范定义在 RFC7252 中。CoAP 协议的产生是为了克服 HTTP 协议在资源受限的物联网设备上的不足。CoAP 协议基于 REST 架构，使用类似于 URL 的资源地址来表示服务器上的资源，并且客户端可以使用类似 HTTP 的 POST、GET、PUT、DELETE 等方法来访问服务器。与 HTTP 相比，CoAP 协议是二进制格式的，比 HTTP 的文本格式更加紧凑，这使得 CoAP 协议更适合于在资源受限的设备上传输数据。

CoAP 协议可以自动解析 CBOR 编码的文件。CoAP 协议支持多种媒体类型，其中包括 CBOR，当 CoAP 协议接收到一个使用 CBOR 编码的文件时，它可以自动解析该文件，并将其转换为可被应用程序处理的数据格式。因此，使用 CoAP 协议搭配 CBOR 编码压缩的隐式证书，可以高效地进行嵌入式设备的身份认证。CoAP 协议结合 CBOR 隐式证书验证具体流程如图 6 所示。

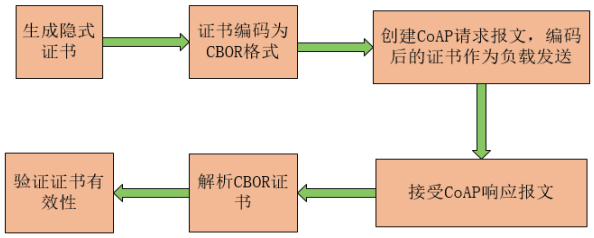

图 6 CoAP 协议隐式证书使用流程图

4 结语

本文针对嵌入式设备通信过程中存在的安全隐患，即在建立安全通信链路之前，需要对设备双方进行身份认证的问题，提出了基于 CBOR 编码的隐式证书压缩方法，利用占用资源更少的 EQCV 隐式证书，以及压缩性更高的 CBOR 二进制编码，对隐式证书进行了进一步的压缩，解决了 PKI 中标准显式证书存在证书过大耗费资源过多的问题，适用于网络计算资源受限的嵌入式设备之间的身份认证。本文对比了通用显式证书、标准 DER 隐式证书、PEM 编码隐式证书以及 CBOR 编码压缩的隐式证书大小，其中 DER 隐式证书约为通用显式证书的 31%，PEM 编码隐式证书虽然可读性高，但证书大小约为通用显式证书的 41.5%，使用 CBOR 编码压缩的隐式证书大小约为显示证书的 24.6%。由于 CoAP 协议可以自动解析 CBOR 编码的文件，使用 CoAP 协议搭配 CBOR 编码压缩的隐式证书，可以高效地进行嵌入式设备的身份认证。

参考文献：

[1] BROWN D R L, GALLANT R, VANSTONE S A. Provably secure implicit certificate schemes[C]//International Conference on Financial Cryptography. Berlin: Springer, 2002:156-165.

[2]CAMPAGNA M.SEC 4: elliptic curve Qu-Vanstone implicit certificate scheme (ECQV)[J]. Standards for efficient cryptography, version, 2013, 1:32.

[3]BARRETO P S L M, JR M A S, RICARDINI J E, et al. Schnorr-based implicit certification: improving the security and efficiency of V2X communications[J]. IACR cryptology eprint archive, 2019,2019:157.

[4] 赵敏，江凌云，李占军 . 基于自签名隐式证书的认证密钥协商协议研究 [J]. 计算机技术与发展 ,2017,27(5):128-132.

[5] 王开轩，滕亚均，王琼霄，等 . 隐式证书的国密算法应用研究 [J]. 信息网络安全 ,2021(5):74-81.

[6] 张群燕，王兵，谯英 . 公钥基础设施 PKI[J]. 科技信息，2006(6):32.

[7]SEC4:Elliptic Curve Qu-Vanstone implicit certificate scheme(ECQV)[EB/OL].[2013-01-24].http://www.secg.org/sec4-1.0.pdf.

[8] 谢冬青 .PEM 标准下密钥的证书管理方式 [J]. 计算机工程与应用 ,2000(4):110-111.

[9]BORMANN C, HOFFMAN P. Concise binary object representation (CBOR)[R]. 2013.

[10] 邓秀兰，饶运涛 .ASN.1 的编解码规则与应用层网络协议开发 [J]. 微计算机信息 ,2004, 20(4):99-100.

[11]HOURIA A, ABDELKADER B M, ABDEREZZAK G.A comparison between the secp256r1 and the koblitz secp256k1 bitcoin curves[J].Indonesian journal of electrical engineering and computer science, 2019,13(3):910-918.

[12]SHELBY Z, HARTKE K, BORMANN C. The constrained application protocol (CoAP)[R]. 2014.

【作者简介】

米轩浩（1995—），男，陕西榆林人，硕士研究生，助理工程师，研究方向：网络安全。

（收稿日期：2024-01-29）