ICS 35.040
L 80
备案号:49741—2015

GM

中华人民共和国密码行业标准

GM/T 0042—2015

三元对等密码安全协议测试规范

Test specification for cryptography and security protocol in tri-element peer architecture

2015-04-01 发布　　2015-04-01 实施

国家密码管理局　　发布

中华人民共和国密码
行业标准
三元对等密码安全协议测试规范
GM/T 0042—2015
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.75 字数 46 千字
2015年6月第一版 2015年6月第一次印刷
*
书号:155066·2-28771 定价 27.00 元

GM/T 0042-2015

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程实验室、国家密码管理局商用密码检测中心、国家无线电监测中心检测中心、中国电信集团公司、中国航天科工集团第二研究院七〇六所、中国电子科技集团公司第十五研究所、国家信息中心、总参第六十一研究所、北京市政务网络管理中心、WAPI 产业联盟、广州杰赛科技股份有限公司、深圳市明华澳汉科技股份有限公司、公安部信息安全等级保护评估中心、北京中电华大电子设计有限责任公司。

本标准主要起草人：曹军、李琴、黄振海、李大为、邓开勇、胡亚楠、宋起柱、高波、孔雷、罗鹏、李国友、李光、吴亚非、杨林、李延春、秦志强、周涛、朱正美、姚蕊、詹葆荣、沈宇超、潘琪、师倩俊、杜志强、颜湘、王月辉、张变玲、铁满霞、张强、张国强、李明、张莎、丁启枫、刘鹊、杨峰、黄丽、潘毅明、童伟刚、王磊等。

引　言

三元对等架构(Tri-element Peer Architecture,TePA)是我国自主提出的普适性网络安全技术架构,其核心技术于2010年6月1日获国际标准化组织ISO/IEC批准发布为国际标准(标准号:ISO/IEC 9798-3:1998/Amd.1:2010),并被批准发布为国家标准(标准号:GB/T 28455—2012)。

三元对等架构是网络与信息安全领域基础共性技术架构,可扩展应用于有线网络、无线移动网络、近距离通信网络、IP安全、数据安全与隐私等多个应用领域,并且支持国家密码管理主管部门认可的密码算法。

本标准的主要目的是针对符合国际标准ISO/IEC 9798-3:1998/Amd.1:2010和国家标准GB/T 15843.3、GB/T 28455—2012的基于三元对等架构的密码安全协议(以下简称三元对等密码安全协议),提出一套测试要求及方法。

本标准是与三元对等架构对应的框架性测试规范,可为三元对等密码安全协议的设计提供参考,提高符合三元对等架构的相关产品的互操作性。

三元对等密码安全协议测试规范

1 范围

本标准规定了三元对等密码安全协议对相关密码算法与安全协议应满足的基本技术要求和对应的测试方法，适用于三元对等密码安全协议相关产品的检测。主要包括如下内容：

a) 密码算法实现的正确性和一致性的技术要求及测试方法；

b) 协议实现的符合性和互操作性的基本技术要求及测试方法。

本标准适用于符合 ISO/IEC 9798-3:1998/Amd.1:2010 和 GB/T 15843.3、GB/T 28455—2012 的设备，用于检测其密码算法和协议实现是否符合上述标准的要求。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 15843.3 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

GB/T 28455—2012 信息安全技术 引入可信第三方的实体鉴别及接入架构规范

GM/T 0002 SM4 分组密码算法

GM/T 0003 SM2 椭圆曲线公钥密码算法

GM/T 0004 SM3 密码杂凑算法

GM/T 0005 随机性检测规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0028 密码模块安全技术要求

GM/T 0039 密码模块安全检测要求

GM/Z 4001 密码术语

CBWIPS/Z 021—2010 无线局域网网络设备标识规范

ISO/IEC 9798-3:1998/Amd.1:2010 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制 补篇1(Information technology—Security techniques—Entity authentication—Part 3: Mechanisms using digital signature techniques—Amendment 1)

3 术语和定义

GM/Z 4001 和 GB/T 28455—2012 所界定的以及下列术语和定义适用于本文件。

3.1

被测设备 tested equipment

实现三元对等密码安全协议的设备。

3.2

测试平台 test platform

提供三元对等密码安全协议测试的平台，用于收集和分析处理测试数据，按照测试规范的要求对测

试数据进行判断，并且对判断结果进行呈现并记录的平台。

3.3

访问控制　access control

按照特定策略，允许或拒绝用户对资源访问的一种机制。

3.4

辅助设备　support equipment

一种特殊的基准设备，除进行三元对等密码安全协议交互外，还需要主动提供用于辅助测试的数据给测试平台。

3.5

基准设备　standard equipment

对被测设备开展测试时需要同步使用的设备，和被测设备协同工作执行三元对等密码安全协议交互过程。基准设备是符合三元对等密码安全协议的设备。

3.6

密码算法　cryptographic algorithm

描述密码处理过程的运算规则。

3.7

密码协议　cryptographic protocol

两个或两个以上参与者使用密码算法，按照约定的规则，为达到某种特定目的而采取的一系列步骤。

3.8

三元对等密码安全协议　cryptography and security protocol in tri-element peer architecture

符合国际标准 ISO/IEC 9798-3：1998/Amd.1：2010 和国家标准 GB/T 15843.3、GB/T 28455—2012 的基于三元对等架构的密码安全协议。

4　符号和缩略语

GM/Z 4001 和 GB/T 28455—2012 界定的以及下列缩略语适用于本文件。

AAC　鉴别访问控制器（Authentication Access Controller）

AS　鉴别服务器（Authentication Server）

IANA　互联网号码分配机构（Internet Assigned Numbers Authority）

OUI　组织唯一性标识（Organizationally Unique Identifier）

PAE　端口访问实体（Port Access Entity）

REQ　请求者（Request）

SMI　管理信息结构（Structure of Management Information）

TAEP　三元鉴别可扩展协议（Tri-element Authentication Extensible Protocol）

TAEPoL　基于链路的三元鉴别可扩展协议（TAEP over Link）

TePA　三元对等架构（Tri-element Peer Architecture）

TePA-AC　基于三元对等架构的访问控制（TePA-based Access Control）

5　基本技术要求

5.1　密码算法实现的正确性和一致性要求

三元对等密码安全协议测试应根据国家密码行业标准的要求，提供密码算法测试所需的输入、输

出，密码算法测试针对三元对等密码安全协议产品中支持的国家密码管理主管部门认可的密码算法。附录D给出了相关密码算法的测试向量。

密码算法的实现应满足：

a) 三元对等密码安全协议中对称密码算法实现的正确性和一致性要求：

三元对等密码安全协议中使用的对称密码算法，其运算结果应与国家密码行业标准中所规定的对应算法提供的标准运算结果一致，包括加密、解密等。

b) 三元对等密码安全协议中非对称密码算法实现的正确性和一致性要求：

三元对等密码安全协议中使用的非对称密码算法，其运算结果应与国家密码行业标准中所规定的对应算法提供的标准运算结果一致，包括加密、解密、密钥交换、签名和验签等。

c) 三元对等密码安全协议中杂凑算法实现的正确性和一致性要求：

三元对等密码安全协议中使用的杂凑算法，其运算结果应与国家密码行业标准中所规定的对应算法提供的标准运算结果一致。

d) 三元对等密码安全协议中密码算法性能要求：

三元对等密码安全协议中使用的密码算法性能应满足产品应用的特定场景需求和国家密码管理相关规定。

5.2 协议实现的符合性和互操作性要求

5.2.1 端口控制要求

三元对等密码安全协议产品中端口访问控制机制应符合GB/T 28455—2012的规定。

GB/T 28455—2012要求端口访问实体(PAE)对鉴别访问控制协议进行操作。对于支持端口访问控制功能的系统，每个端口都存在PAE，无论该系统扮演请求者角色还是鉴别访问控制器角色。在鉴别交互中请求者PAE和鉴别访问控制器PAE均根据鉴别过程的结果控制受控端口的授权/未授权状态。

在鉴别成功完成之前，请求者和鉴别访问控制器通过非受控端口进行鉴别交互，或者访问对方提供的没有访问控制限制的处于非受控端口上的服务。一旦鉴别成功完成，两个系统均允许对方访问其受控端口提供的服务。

5.2.2 TAEP协议封装要求

三元对等密码安全协议中鉴别协议的数据封装应满足GB/T 28455—2012中定义的TAEP协议的封装要求。

TAEP Request和Response分组格式中的Type字段用于表示Request和Response分组的类型，定义参见附录A。

5.2.3 链路上的TAEP封装(TAEPoL)协议要求

GB/T 28455—2012定义了请求者PAE和鉴别访问控制器PAE之间负载TAEP分组的封装技术。该封装为链路上的TAEP记为TAEPoL。TAEPoL协议使用0x891b的以太类型字段。

5.2.4 底层、传输层协议封装要求

在鉴别访问控制器和鉴别服务器之间传递TAEP消息使用GB/T 28455—2012中所规范的TAEP-AS-SVC服务协议，鉴别服务器作为服务端在UDP/TCP端口5111上接收TAEP消息，鉴别访问控制器作为客户端发送TAEP消息。

5.3 其他要求

产品需考虑自检，且产品可靠性、稳定性应满足产品应用的特定场景需求。

根据协议在产品中的实现可提供算法实现正确性以及随机数自检说明。

产品中的密码模块的安全要求应满足 GM/T 0028。

6 测试环境要求

6.1 测试设备

测试设备应经计量检定，并在检定有效期内，测试设备的精度应满足测量要求。

测试机构提供辅助设备和测试平台。

辅助设备和被测设备需按要求向测试平台提供测试数据。

6.2 测试拓扑

6.2.1 概述

三元对等密码安全协议所涉及的协议实体包括请求者 REQ、鉴别访问控制器 AAC 和鉴别服务器 AS。三元对等密码安全协议测试拓扑中除测试平台外，还有三种测试角色：被测设备、基准设备、辅助设备。开展测试时，由被测设备和辅助设备提供测试数据。协议实体与测试角色的对应关系如表 1 所示：

表 1 协议实体与测试角色的对应关系

被测设备	基准设备	辅助设备(可选)
REQ	AAC	AS
AAC	REQ	AS
AS	无	无

6.2.2 REQ 测试拓扑

针对 REQ 的测试拓扑中，被测设备为 REQ，基准设备为 AAC，辅助设备为 AS。

辅助设备 AS 和基准设备 AAC 连接，基准设备 AAC 与被测设备 REQ 连接；由辅助设备 AS 和被测设备 REQ 将收发的数据按要求提供给测试平台。

在 REQ 测试中，被测设备 REQ 要支持外部输入公私钥或支持配置文件方式导入，具体方式本标准中不予限定，REQ 测试拓扑如图 1 所示：

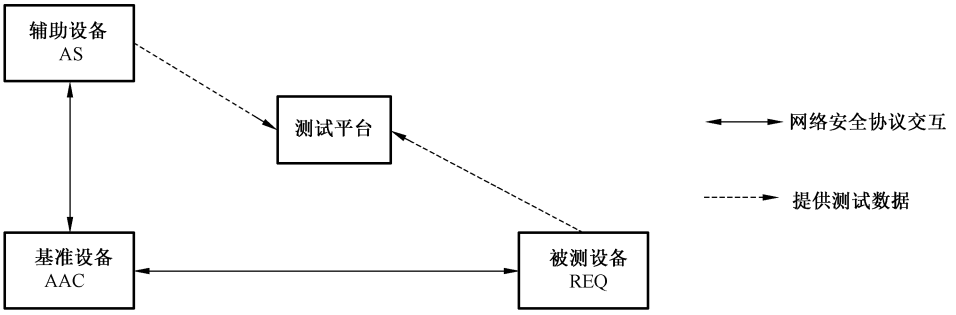

图 1　REQ 测试拓扑

6.2.3　AAC 测试拓扑

针对 AAC 的测试拓扑中，被测设备为 AAC，基准设备为 REQ，辅助设备为 AS。

辅助设备 AS 和被测设备 AAC 连接，基准设备 REQ 与被测设备 AAC 连接；由辅助设备 AS 和被测设备 AAC 将收发的数据按要求提供给测试平台。

在 AAC 测试中，被测设备 AAC 要支持外部输入公私钥或支持配置文件方式导入，具体方式本标准中不予限定，AAC 测试拓扑如图 2 所示：

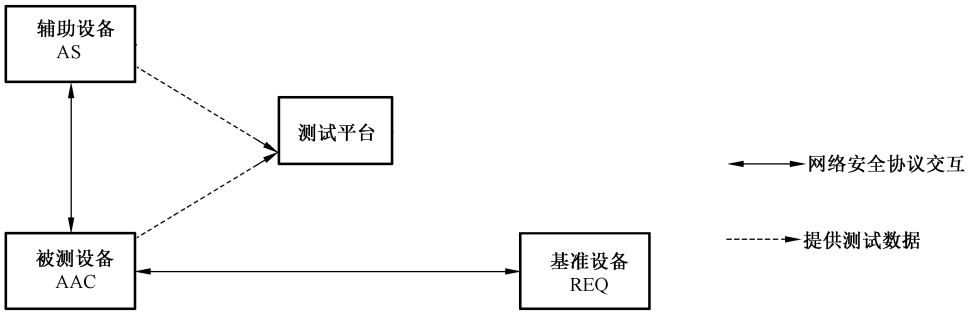

图 2　AAC 测试拓扑

6.2.4　AS 测试拓扑

针对 AS 的测试拓扑中，被测设备为被测 AS，基准设备无，辅助设备无。

被测设备 AS 和测试平台连接，由测试平台模拟 AAC 以及 REQ 和被测设备 AS 进行交互，由被测设备 AS 将收发的数据按要求提供给测试平台，AS 测试拓扑如图 3 所示：

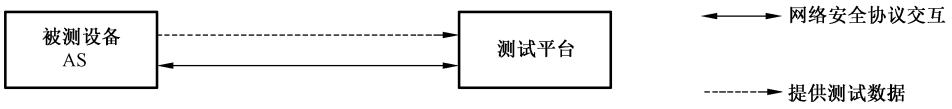

图 3　AS 测试拓扑

7　三元对等密码安全协议测试统一封装

7.1　统一封装数据结构定义

辅助设备和被测设备应按照本章定义的三元对等密码安全协议测试统一封装结构将原始消息进行

封装后提供给测试平台。三元对等密码安全协议测试统一封装数据结构定义如图4所示：

图4　三元对等密码安全协议测试统一封装

其中：

——版本字段，长度为1个八位位组，其值表示三元对等密码安全协议测试统一封装的版本号，当前版本为1；其他值保留；

——设备角色字段，长度为1个八位位组，其值表示三元对等密码安全协议测试统一封装数据的构造设备的角色，其中：0表示REQ；1表示AAC；2表示AS；其他值保留；

——收发标识字段，长度为1个八位位组，其中比特0有意义，其值表示使用三元对等密码安全协议测试统一封装所封装的原始消息是提供该封装数据的设备收到的数据还是发出的数据，比特0取值为0表示收到的数据，比特0取值为1表示发出的数据；比特1～7保留；

——厂商标识字段，长度为4个八位位组，其值表示设备厂商的Vendor ID，高位八位位组为00，低位三个八位位组使用网络字节顺序的由IANA分配给厂商的SMI网络管理专用企业代码，如企业没有该代码，可使用00-00-00；

——长度字段，长度为2个八位位组，其值表示三元对等密码安全协议测试统一封装所有字段的八位位组数；

——鉴别套件字段，长度为4个八位位组由3个八位位组的OUI和1个八位位组的套件类型组成，本标准中定义套件如表2所示：

表2　鉴别管理套件

OUI 3个八位位组	类型 1个八位位组	含义
00-14-72	0	保留
00-14-72	1	基于证书鉴别
00-14-72	2	基于预共享密钥鉴别
00-14-72	3～255	保留
其他	0～255	保留

——协议类型字段，长度为1个八位位组，其值表示所封装的TAEP协议的类型，取值同GB/T 28455—2012中定义的TAEP协议中的TYPE字段；取值参见附录A；

——分组序号字段，长度为 2 个八位位组，其值表示协议分组序号；第一个分组序号为 1，后序分组依次按 1 递增；

——分片序号字段，长度为 2 个八位位组，其值表示分片的顺序编号，每一个分组的第一个分片序号为 0，后序分片依次按 1 递增；

——分片标识字段，长度为 1 个八位位组，比特 0 有意义，表示后续是否有分片，比特 0 取值为 0 表示没有，取值为 1 表示有；比特 1～7 保留；

——扩展字段，长度为 5 个八位位组，保留；

——数据字段，长度可变。

7.2 统一封装数据元素定义

统一数据封装中的数据字段中的数据元素采用 TLV 格式封装，如图 5 所示：

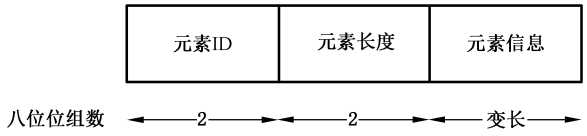

图 5 TLV 数据封装

其中：

——元素 ID 字段，长度为 2 个八位位组，其值表示三元对等密码安全协议测试统一封装的元素类型，具体定义见附录 B；

——元素长度字段，长度为 2 个八位位组，其值表示元素信息字段的八位位组数；

——元素信息字段，长度由元素长度字段指定，其值表示数据元素的内容。

统一数据封装中的数据字段中的数据元素的元素 ID、元素长度、元素信息等定义见附录 B。

8 密码算法实现的正确性和一致性测试方法

8.1 对称密码算法实现的正确性和一致性测试方法

测试方法如下：

a) 搭建测试网络，被测设备、基准设备和辅助设备执行三元对等密码安全协议交互；

b) 被测设备和辅助设备将三元对等密码安全协议交互过程中接收和发送的交互消息涉及对称密码算法的相关数据信息以及已知的相关数据，按照 7.1 定义的三元对等密码安全协议测试统一封装进行封装提交给测试平台；

c) 测试平台解析得到对称密码算法测试相关的数据字段，并利用这些字段开展对称密码算法实现的正确性和一致性测试，其中对 SM4 算法的测试见 GM/T 0002。

8.2 数字签名算法实现的正确性和一致性测试方法

测试方法如下：

a) 搭建测试网络，被测设备、基准设备和辅助设备执行三元对等密码安全协议交互；

b) 被测设备和辅助设备将三元对等密码安全协议交互过程中接收和发送的交互消息涉及数字签名算法的相关数据信息以及已知的相关数据，按照 7.1 定义的三元对等密码安全协议测试统一封装进行封装提交给测试平台；

c) 测试平台解析得到数字签名算法测试相关的数据字段，并利用这些字段开展数字签名算法实现的正确性和一致性测试，其中对 SM2 数字签名算法的测试见 GM/T 0003、GM/T 0009。

8.3 密钥交换协议实现的正确性和一致性测试方法

测试方法如下：

a) 搭建测试网络，被测设备、基准设备和辅助设备执行三元对等密码安全协议交互；

b) 被测设备和辅助设备将三元对等密码安全协议交互过程中接收和发送的交互消息涉及密钥交换协议的相关数据信息以及已知的相关数据，按照 7.1 定义的三元对等密码安全协议测试统一封装进行封装提交给测试平台；

c) 测试平台解析得到密钥交换协议测试相关的数据字段，并利用这些字段开展密钥交换协议实现的正确性和一致性测试，其中对 SM2 密钥交换协议的测试见 GM/T 0003、GM/T 0009。

8.4 公钥加密算法实现的正确性和一致性测试方法

测试方法如下：

a) 搭建测试网络，被测设备、基准设备和辅助设备执行三元对等密码安全协议交互；

b) 被测设备和辅助设备将三元对等密码安全协议交互过程中接收和发送的交互消息涉及公钥加密算法的相关数据信息以及已知的相关数据，按照 7.1 定义的三元对等密码安全协议测试统一封装进行封装提交给测试平台；

c) 测试平台解析得到公钥加密算法测试相关的数据字段，并利用这些字段开展公钥加密算法实现的正确性和一致性测试，其中对 SM2 加密算法的测试见 GM/T 0003、GM/T 0009。

8.5 数字证书格式测试方法

测试方法如下：

a) 搭建测试网络，被测设备、基准设备和辅助设备执行三元对等密码安全协议交互；

b) 被测设备和辅助设备将三元对等密码安全协议交互过程中接收和发送的交互消息涉及数字证书格式的相关数据信息以及已知的相关数据，按照 7.1 定义的三元对等密码安全协议测试统一封装进行封装提交给测试平台；

c) 测试平台解析得到数字证书格式测试相关的数据字段，并利用这些字段开展数字证书格式测试，其中对 SM2 数字证书格式的测试见 GM/T 0015。

8.6 密码杂凑算法测试方法

测试方法如下：

a) 搭建测试网络，被测设备、基准设备和辅助设备执行三元对等密码安全协议交互；

b) 被测设备和辅助设备将三元对等密码安全协议交互过程中接收和发送的交互消息涉及密码杂凑算法的相关数据信息以及已知的相关数据，按照 7.1 定义的三元对等密码安全协议测试统一封装进行封装提交给测试平台；

c) 测试平台解析得到密码杂凑算法测试相关的数据字段，并利用这些字段开展密码杂凑算法实现的正确性和一致性测试，其中对 SM3 密码杂凑算法的测试见 GM/T 0004。

8.7 随机数测试方法

测试方法如下：

a) 搭建测试网络，被测设备、基准设备和辅助设备执行三元对等密码安全协议交互；

b) 被测设备和辅助设备将三元对等密码安全协议交互过程中接收和发送的交互消息涉及随机数的相关数据信息以及已知的相关数据，按照 7.1 定义的三元对等密码安全协议测试统一封装进行封装提交给测试平台；

c) 测试平台解析得到随机数测试相关的数据字段，并利用这些字段按照 GM/T 0005 要求提取随机数样本，并按照 GM/T 0005 的相关要求进行检测。

9 协议实现一致性和互操作性测试方法

9.1 端口控制测试方法

该项测试针对 REQ 和 AAC。

当被测设备为 REQ 时，测试拓扑见 6.2.2，需要基准设备 AAC、辅助设备 AS 开展测试：

a) 搭建测试网络，被测设备、基准设备和辅助设备执行三元对等密码安全协议交互；

b) 为被测设备 REQ 颁发并安装合法证书；为基准设备 AAC 颁发并安装非法证书；

c) 检查被测设备 REQ 的受控端口在鉴别完成前和鉴别完成后的状态是否符合 GB/T 28455—2012 的要求；

d) 为被测设备 REQ 颁发并安装合法证书；为基准设备 AAC 颁发并安装合法证书；

e) 检查被测设备 REQ 的受控端口在鉴别完成前和鉴别完成后的状态是否符合 GB/T 28455—2012 的要求。

当被测设备为 AAC 时，测试拓扑见 6.2.3，需要基准设备 REQ、辅助设备 AS 开展测试：

a) 搭建测试网络，被测设备、基准设备和辅助设备执行三元对等密码安全协议交互；

b) 为被测设备 AAC 颁发并安装合法证书；为基准设备 REQ 颁发并安装非法证书；

c) 检查被测设备 AAC 的受控端口在鉴别完成前和鉴别完成后的状态是否符合 GB/T 28455—2012 的要求；

d) 为被测设备 AAC 颁发并安装合法证书；为基准设备 REQ 颁发并安装合法证书；

e) 检查被测设备 AAC 的受控端口在鉴别完成前和鉴别完成后的状态是否符合 GB/T 28455—2012 的要求。

9.2 TAEP 协议封装测试方法

该项测试针对 REQ、AAC、AS。

a) 搭建测试网络，被测设备、基准设备和辅助设备执行三元对等密码安全协议交互；

b) 检查被测设备发出的数据的封装是否符合 GB/T 28455—2012 中定义的 TAEP 协议封装的要求。

9.3 TAEPoL 协议封装测试方法

该项测试针对 REQ 和 AAC。

a) 搭建测试网络，被测设备、基准设备和辅助设备执行三元对等密码安全协议交互；

b) 检查被测设备发出的数据的封装是否符合 GB/T 28455—2012 中定义的 TAEPoL 协议封装的要求。

9.4 TCP/UDP 端口测试方法

该项测试针对 AAC 和 AS。

当被测设备为 AAC 时，需要基准设备 REQ、辅助设备 AS 开展测试：

a) 搭建测试网络，被测设备、基准设备和辅助设备执行三元对等密码安全协议交互；

b) 检查被测设备发给 AS 的数据是否是发送到 GB/T 28455—2012 中规定的 TCP/UDP 端口。

当被测设备为 AS 时，不需要基准设备和辅助设备：

a) 将被测设备与测试平台连通，由测试平台模拟 AAC 设备与被测设备执行三元对等密码安全协议交互；

b) 检查被测设备发出的数据是否通过 GB/T 28455—2012 中规定的 TCP/UDP 端口发出。

附 录 A
（资料性附录）
TAEP 协议封装 Request 和 Response 分组 Type 定义

TAEP Request 和 Response 分组格式中的 Type 字段定义见 GB/T 28455—2012，其中已分配的 Type 字段定义如表 A.1 所示。

表 A.1 Request 和 Response 分组类型定义

Type 值	定义	描述
0	保留	
1	Identity	用于鉴别访问控制器询问请求者的身份
2	Notification	用于将一个可显示的消息从鉴别访问控制器传递到请求者
3	Nak (Response only)	用于表示不支持 Request 分组中提议的鉴别方法
4	AKE	鉴别密钥协商协议
5	NEAU-A	使用非对称密码算法的 NEAU 协议
6	TSSI	基于三元对等安全架构的传感器网络安全基础设施
7	WSAI	WPAN 安全接入基础设施
8～197	保留	
198	TRAIS-P	基于公钥密码算法的 TRAIS 协议
199	MPAS-P	基于公钥密码算法的 MPAS 协议
200	TAEP-WAI	TCA 中 TAEP 封装 WAPI 协议单播密钥协商
201	TAEP-PAI	TCA 中 TAEP 封装 PAI 协议
202	TAEP-TTLS	TCA 中 TAEP 封装完全匿名模式作为隧道方法时的 TLS 协议
203	TAEP-IRS	TCA 中封装平台修补数据
204～237	保留	
238	TPA(EPON)	标识 TPSec 协议中 TPA 协议
239	TSKSA(11Z)	标识 TDLS 站间密钥安全关联是使用 WAPI 对 TDLS 进行保护
240	TAI	标识 TISec 协议中 TAI 协议
241	TAAA	标识宽带无线多媒体空中接口标准中的鉴别与密钥管理协议
242	WACA	标识无线局域网自动配置与接入技术中的注册协议
243	Neighbor SW Negotiation	TLSec 邻居交换设备选择协议，见 GB/T 15629.3—2014
244	Neighbor information	TLSec 邻居节点发现协议，见 GB/T 15629.3—2014
245	TAEP-CAAP	TLSec 证书鉴别协议，见 GB/T 15629.3—2014
246	Policy Negotiation	TLSec 安全策略协商协议，见 GB/T 15629.3—2014
247	SW Routing Seek	TLSec 交换路径探寻协议，见 GB/T 15629.3—2014
248	TAEP-IBAP	TAEP-IBAP 是基于身份签名机制的鉴别协议，见 GB/T 28455—2012 附录 B
249	TAEP-CBAP	TAEP-CBAP 是基于三实体公钥的鉴别协议，见 GB/T 28455—2012 附录 B
250	TP Authentication	用于鉴别访问控制器向鉴别服务器询问可用的鉴别方法
251～253	保留	
254	Expanded Types	用来支持厂商自定义
255	Experimental use	用于测试新的 TAEP 鉴别协议类型

附 录 B
（规范性附录）
三元对等密码安全协议测试统一封装数据元素

B.1 三元对等密码安全协议测试统一封装数据元素 ID 定义

三元对等密码安全协议测试统一封装数据元素 ID 定义如表 B.1 所示。

表 B.1 三元对等密码安全协议测试统一封装数据元素 ID 定义

元素 ID	字段	长度（八位位组）	意义
0			保留
1	DST_IP	变长	目的 IP 地址
2	SRC_IP	变长	源 IP 地址
3	DA	6	目的地址
4	SA	6	源地址
5	EtherType	2	以太类型字段
6	Code	1	Code 编码
7	Identifier	1	匹配标识
8	Port_Num	2	端口号
9	Port_Status	1	端口控制状态
10	TAEP_Type	1	TAEP 类型
11	Message_Type	1	消息类型
12	Symmetric_Encryption_Testdata	变长	对称密码算法加密测试数据
13	Symmetric_Integrity_Testdata	变长	对称密码算法完整性测试数据
14	Asymmetric_Encryption_Testdata	变长	公钥加密测试数据
15	KeyExchange_Testdata	变长	密钥交换测试数据
16	Signature_Testdata	变长	签名算法测试数据
17	MAC_Testdata	变长	消息鉴别码算法测试数据
18	KD_Testdata	变长	密钥导出算法测试数据
19	N_{REQ}	32	REQ 随机数
20	N_{AAC}	32	AAC 随机数
21	N_{AS}	32	AS 随机数
22	$Cert_{REQ}$	变长	REQ 证书
23	$Cert_{AAC}$	变长	AAC 证书
24	$Cert_{AS}$	变长	AS 证书

表 B.1（续）

元素 ID	字段	长度（八位位组）	意义
25	Res_{REQ}	1	REQ 证书验证结果
26	Res_{AAC}	1	AAC 证书验证结果
27	$AccRes_{REQ}$	1	REQ 接入结果
28	$AccRes_{AAC}$	1	AAC 接入结果
29～65534			保留
65535	Original_Message	可变	原始消息

B.2 数据元素中字段定义

B.2.1 目的 IP 地址

DST_IP：目的 IP 地址字段，表示该帧对应的原始消息发往的目的 IP 地址，由 2 个八位位组的长度字段和变长的内容字段表示；长度字段表示内容字段的八位位组数，内容字段为目的 IP 地址取值。

B.2.2 源 IP 地址

SRC_IP：源 IP 地址字段，表示该帧对应的原始消息发送方的 IP 地址，由 2 个八位位组的长度字段和变长的内容字段表示；长度字段表示内容字段的八位位组数，内容字段为源 IP 地址取值。

B.2.3 目的地址

DA：目的地址字段，标识该帧对应的原始消息发往的目的地的 MAC 地址，取值为 TAEPoL 分组中的 DA 字段。

B.2.4 源地址

SA：源地址字段，标识发送该帧对应的原始消息的站的 MAC 地址，取值为 TAEPoL 分组中的 SA 字段。

B.2.5 以太类型字段

EtherType：以太类型字段，标识该帧对应的原始消息封装所使用的以太类型字段，取值为 TAEPoL 分组中的 EtherType 字段。

B.2.6 Code 编码

Code：Code 编码字段，定义见 GB/T 28455—2012，标识该帧对应的原始消息的 TAEP 分组类型，取值为 TAEP 分组中的 code 字段。

B.2.7 匹配标识

Identifier：匹配标识，定义见 GB/T 28455—2012，用于匹配 TAEP Request 分组和 Response 分组，取值为 TAEP 分组中 Identifier 字段值。

B.2.8 端口号

Port_Num：端口号字段，标识该帧对应的原始消息传输所使用的 UDP/TCP 端口号。

B.2.9 端口控制状态

Port_Status：端口控制状态字段；比特 0 有效，比特 0 标识设备对应的受控端口的状态信息，比特 0 取值为 1 表示受控端口连通，数据可以通过受控端口；取值为 0 表述受控端口关闭，数据不可以通过受控端口。

B.2.10 TAEP 类型

TAEP_Type：TAEP 类型字段，定义见 GB/T 28455—2012，标识该帧对应的原始消息使用 TAEP 封装时的 Request 和 Response 分组的类型值。

B.2.11 消息类型

Message_Type：消息分组类型字段，根据对应的 TAEP Type 值/Key Descriptor 类型值不同在每个三元对等密码安全协议中进行说明，取值为 TAEP 封装的消息的 MessageType 字段值或者是 Sub-Type 字段值，用于标识不同的分组消息。

B.2.12 对称密码算法加密测试数据

Symmetric_Encryption_Testdata：对称密码算法加密测试数据字段，由对称密码算法标识、加密密钥、IV、加密对象明文、加密对象密文组成；其中：

——Encrypt_Algorithm_Flag，对称密码算法标识字段，长度为 1 个八位位组，标识所使用的对称密码算法及模式，字段定义同对称密码算法及模式字段；

——Encrypt_KeyInfo，加密密钥字段，标识对称密码算法加密时所使用的密钥，长度可变，字段定义同密钥字段；

——IV，初始化向量，长度可变，标识特定加密模式下使用的初始化向量，字段定义同数据字段；

——EncryptObject_Plaintext，加密对象明文字段，长度可变，标识加密所保护的对象的明文数据信息，字段定义同数据字段；

——EncryptObject_Ciphertext，加密对象密文字段，长度可变，标识加密所保护的对象的加密后的密文数据信息，字段定义同数据字段。

相关字段定义如下：

a) 对称密码算法及模式字段：长度为 1 个八位位组，1 表示 SM4-GCM 算法，2 表示 SM4-CTR 算法，3 表示 SM4-OFB 算法，4 表示 SM4-CBC，5 表示 SM4-ECB，其他值保留；其中 SM4 算法见 GM/T 0002；

b) 密钥字段：长度可变，由 2 个八位位组长度的长度字段、可变长度的密钥内容字段组成；其中长度字段表示密钥内容字段的八位位组数，密钥内容字段表示密钥值；

c) 数据字段：长度可变，由 2 个八位位组长度的长度字段、可变长度的内容字段组成；其中长度字段表示内容字段的八位位组数，内容字段即数据内容。

B.2.13 对称密码算法完整性测试数据

Symmetric_Integrity_Testdata：对称密码算法完整性测试数据字段，由完整性算法标识、完整性计算密钥、完整性保护对象明文、消息完整性校验值组成；其中：

——MIC_Algorithm_Flag，完整性算法标识字段，长度为 1 个八位位组，标识计算消息完整性时所

使用的对称密码算法及模式，字段定义同对称密码算法及模式字段，见 B.2.12；

——MIC_KeyInfo，完整性计算密钥字段，长度可变，标识计算消息完整性时使用的密钥，字段定义同密钥字段，见 B.2.12；

——MICObject_PlainText，完整性保护对象明文字段，长度可变，标识消息完整性值所保护的对象的明文数据信息，字段定义同数据字段，见 B.2.12；

——MIC，消息完整性校验值字段，长度可变，由 2 个八位位组长度的长度字段和可变长度的内容字段组成；其中长度字段表示内容字段的八位位组数，内容字段即消息完整性校验的值。

B.2.14 公钥加密测试数据

Asymmetric_Encryption_Testdata：公钥加密测试数据字段，由公钥加密密码算法标识、公钥算法曲线参数、密码杂凑算法标识、加密公钥、加密对象明文、加密对象密文组成；其中：

——Encrypt_Algorithm_Flag，公钥加密密码算法标识字段，长度为 1 个八位位组，标识所使用的公钥密码算法；其中 1 表示 SM2 加密，其他值保留；其中 SM2 加密算法见 GM/T 0003；

——CurvePara，公钥算法曲线参数字段，标识所使用的曲线的信息，长度可变，由 2 个八位位组的长度字段、可变长度的曲线 OID 字段组成；其中长度字段表示曲线 OID 字段的八位位组数，曲线 OID 字段用 ASN.1 编码；

——Hash_Algorithm_Flag，密码杂凑算法标识字段，长度为 1 个八位位组，标识公钥加密时所使用的密码杂凑算法；其中 0 表示无，1 表示 SM3 算法，2 表示 SHA256，其他值保留；其中 SM3 算法见 GM/T 0004；

——Encrypt_KeyInfo，加密公钥字段，长度可变，标识公钥加密时所使用的密钥，字段定义同密钥字段，见 B.2.12；

——EncryptObject_Plaintext，加密对象明文字段，长度可变，标识加密所保护的对象的明文数据信息，字段定义同数据字段，见 B.2.12；

——EncryptObject_Ciphertext，加密对象密文字段，长度可变，标识加密所保护的对象的加密后的密文数据信息，字段定义同数据字段，见 B.2.12。

B.2.15 密钥交换测试数据

KeyExchange_Testdata：密钥交换测试数据字段，由密钥交换算法标识、公钥算法曲线参数、密码杂凑算法标识、对端密钥交换公钥、本地密钥交换公钥、对端临时公钥、本地临时公钥、对端随机数、本地随机数、对端 ID、本地 ID、密钥交换输出密钥组成；其中：

——KeyExchange _Algorithm_Flag，密钥交换算法标识字段，长度为 1 个八位位组，标识所使用的密钥交换算法；其中 1 表示 SM2 密钥交换算法，其他值保留；其中 SM2 密钥交换算法见 GM/T 0003；

——CurvePara，公钥算法曲线参数字段，字段定义见 B.2.14；

——Hash_Algorithm_Flag，密码杂凑算法标识字段，标识密钥交换时所使用的哈希算法，字段定义见 B.2.14；

——Peer_DHPublicKeyInfo，对端密钥交换公钥，标识对端设备用于密钥交换时的公钥信息，字段定义同密钥字段，见 B.2.12；

——Local_DHPublicKeyInfo，本地密钥交换公钥，标识本地设备用于密钥交换时的公钥信息，字段定义同密钥字段，见 B.2.12；

——Peer_Temporary_DHPublicKeyInfo，对端临时公钥，标识对端设备用于密钥交换时的临时公钥信息，字段定义同密钥字段，见 B.2.12；

——Local_Temporary_DHPublicKeyInfo，本地临时公钥，标识本地设备用于密钥交换时的临时公

钥信息，字段定义同密钥字段，见 B.2.12；

——Peer_Random_Number，对端随机数，字段定义同随机数字段；

——Local_Random_Number，本地随机数，字段定义同随机数字段；

——PeerID，对端 ID，标识对端设备身份 ID，字段定义同设备 ID 字段；

——LocalID，本地 ID，标识本地设备身份 ID，字段定义同设备 ID 字段；

——KeyExchange_KeyInfo，密钥交换输出密钥字段，长度可变，标识密钥交换算法最终的输出密钥，字段定义同密钥字段，见 B.2.12。

相关字段定义如下：

a) 随机数字段，长度可变，由 2 个八位位组的长度字段、可变长度的内容字段构成，其中：长度字段表示内容字段的八位位组数，内容字段为随机数值；

b) 设备 ID 字段，长度可变，由 2 个八位位组的身份标识字段、2 个八位位组的长度字段、可变长度的内容字段构成，其中：身份标识字段，表示身份类型，取值为 1 表示后面的内容字段是由 X.509 V3 证书的持有者名称、颁发者名称、序列号字段组成；其他值保留；长度字段表示内容字段的八位位组数，内容字段定义由身份标识字段确定。

B.2.16 签名算法测试数据

Signature_Testdata：签名算法测试数据字段，由签名算法标识、公钥算法曲线参数、密码杂凑算法标识、签名保护对象、签名组成；其中：

——Signature_Algorithm_Flag，签名算法标识字段，长度为 1 个八位位组，标识所使用的签名算法；其中 1 表示 SM2 签名，其他值保留；其中 SM2 签名算法见 GM/T 0003；

——CurvePara，公钥算法曲线参数字段，标识所使用的曲线的信息，字段定义见 B.2.14；

——Hash_Algorithm_Flag，密码杂凑算法标识字段，标识签名时所使用的密码杂凑算法，字段定义见 B.2.14；

——LocalID，本地 ID，标识本地设备身份 ID，字段定义同设备 ID 字段，见 B.2.15；

——SignatureObject，签名保护对象字段，标识签名所保护的对象的数据信息，字段定义同数据字段，见 B.2.12；

——SignatureValue，签名字段，长度可变，标识签名信息，由 2 个八位位组的签名长度字段和可变长度的签名内容字段组成，其中签名长度字段标识签名内容字段的八位位组数，签名内容字段为签名的值，将签名结果转化成的八位位组串。

B.2.17 消息鉴别码算法测试数据

MAC_Testdata：消息鉴别码算法测试数据字段，由消息鉴别码算法标识、消息鉴别密钥、消息鉴别码保护对象、消息鉴别码组成；其中：

——MAC_Algorithm_Flag，消息鉴别码算法标识字段，长度为 1 个八位位组，标识所使用的签名算法；其中 1 表示 HMAC-SM3，2 表示 HMAC-SHA256；其他值保留；SM3 算法见 GM/T 0004；

——MAC_KeyInfo，消息鉴别密钥，长度可变，标识计算消息鉴别码所使用的密钥信息，字段定义同密钥字段，见 B.2.12；

——MAC_Object，消息鉴别码保护对象字段，长度可变，标识消息鉴别码所保护的对象的数据信息，字段定义同数据字段，见 B.2.12；

——MACValue，消息鉴别码字段，长度可变，标识消息鉴别码信息，由 2 个八位位组的消息鉴别码长度字段和可变长度的消息鉴别码内容字段组成，其中消息鉴别码长度字段标识消息鉴别码内容字段的八位位组数，消息鉴别码内容字段为消息鉴别码的值。

B.2.18 密钥导出算法测试数据

KD_Testdata：密钥导出算法测试数据字段，由密钥导出算法标识、密钥导出输入公钥、密钥导出输入字符串、密钥导出输出密钥组成；其中：

——KD_Algorithm_Flag，密钥导出算法标识字段，长度为 1 个八位位组，标识所使用的密钥导出算法；其中 1 表示 KD-HMAC-SM3，2 表示 KD-HMAC-SHA256；其他值保留；SM3 算法见 GM/T 0004；

——KD_KeyInfo，密钥导出输入密钥，长度可变，标识进行密钥导出时所输入的密钥种子，字段定义同密钥字段，见 B.2.12；

——KD_Text，密钥导出输入字符串，长度可变，标识进行密钥导出时所输入的字符串信息，字段定义同数据字段，见 B.2.12；

——KD_OutputKeyInfo，密钥导出输出密钥字段，长度可变，标识利用密钥输出的密钥信息，定义同密钥字段，见 B.2.12。

B.2.19 REQ 随机数

N_{REQ}：表示 REQ 随机数，字段定义同随机数字段，见 B.2.15。

B.2.20 AAC 随机数

N_{AAC}：表示 AAC 随机数，字段定义同随机数字段，见 B.2.15。

B.2.21 AS 随机数

N_{AS}：表示 AS 随机数，字段定义同随机数字段，见 B.2.15。

B.2.22 REQ 证书

$Cert_{REQ}$：表示 REQ 证书，取值为 TAEP 分组中 REQ 的证书；定义同证书字段。

其中：证书字段，长度可变，由 2 个八位位组的证书标识字段、2 个八位位组的证书长度字段以及可变长度的证书数据字段组成；其中证书标识字段表示证书类型，1 表示该字段的证书数据为 X.509_PEM_SM2 证书、2 表示该字段的证书数据为 X.509_PKCS＃12_SM2 证书，其余值保留；证书长度字段为证书数据字段的八位位组数；证书数据字段为证书的内容。其中证书中涉及的设备命名格式见 CBWIPS/Z 021—2010，设备标识见附录 C。

B.2.23 AAC 证书

$Cert_{AAC}$：表示 AAC 证书，取值为 TAEP 分组中 AAC 的证书，字段定义同证书字段，见 B.2.22。

B.2.24 AS 证书

$Cert_{AS}$：表示 AS 证书，取值为 TAEP 分组中 AS 的证书，字段定义同证书字段，见 B.2.22。

B.2.25 REQ 证书验证结果

Res_{REQ}：表示 REQ 证书验证结果，同证书结果字段。

其中：证书结果字段，长 1 个八位位组，0 表示证书有效；1 表示证书的颁发者不明确；2 表示证书基于不可信任的根证书；3 表示证书未到生效期或已过期；4 表示签名错误；5 表示证书已吊销；6 表示证书未按规定用途使用；7 表示证书吊销状态未知；8 表示证书错误原因未知；其他值保留。

B.2.26 AAC 证书验证结果

RES_{AAC}：表示 AAC 证书验证结果，字段定义同证书结果字段，见 B.2.25。

B.2.27 REQ 接入结果

$AccRes_{REQ}$：表示 REQ 接入结果，字段定义同接入结果字段；

其中：接入结果字段，长 1 个八位位组，0 表示接入成功，对应证书验证结果值为 0；1 表示无法验证证书，对应证书验证结果值为 1；2 表示证书错误，对应证书验证结果除 0 和 1 之外的其他值；3 表示本地策略禁止；其他值保留。

B.2.28 AAC 接入结果

$AccRes_{AAC}$：表示 AAC 接入结果，字段定义同接入结果字段，见 B.2.27。

B.2.29 原始消息

Original_Message：原始消息字段，表示三元对等密码安全协议测试统一封装所封装的原始消息，由 2 个八位位组长度的消息类型，2 个八位位组长度的消息长度，可变长度的消息内容构成；其中：消息类型字段标识消息的类型，1 表示为 TAEP-Packet 帧，2 表示为 TAEPoL-Key 帧，其他值保留；消息长度字段表示消息内容的八位位组数。

附 录 C
（规范性附录）
设备命名

证书中的设备命名规则见 CBWIPS/Z 021—2010 定义。其中强制域为 TLV 格式的字符串，取值为“HUFU”＋掩码字符串 FLAG；其中掩码字符串 FLAG 取值为如下二进制数 FLAG 对应的十进制数作为字符串；二进制数 FLAG 定义如表 C.1 所示。

表 C.1 证书强制域二进制数 FLAG

比特	协议	含义
0	HUFU	通用
1	TTS	传输控制协议(TCP)安全
2	TLSec	有线局域网(LAN)安全
3	TPSec	无源光网络(xPON)安全
4	TPLS	电力线通信(PLC)安全
5	EACI	同轴电缆(EoC)安全
6	WAPI 1.0	无线局域网(WLAN)安全 1.0
7	WAPI 2.0	无线局域网(WLAN)安全 2.0
8	TAAA	无线城域网(WMAN)安全
9	TMSS	LTE(4G)安全
10	TRAIS	射频识别(RFID)安全
11	NEAU	近场通信(NFC)安全
12	MPAS	移动支付安全
13	TSSI	传感网(WSN)安全
14	WSAI	无线个域网(WPAN)安全
15	EFHP	超宽带(UWB)安全
16	MSAI	磁域网(MFAN)安全
17	TISec	IP 安全
18	EVSec	语音安全
19	TAEA	匿名技术
20	TCA	可信连接
21	EIDSA	网络电子身份证(EID)安全
其余	保留	

需要说明的是：

a) 比特 0 为特殊标识位，比特 0 置 1 时，其他比特置 0；即强制域为“HUFU1”表示该证书可通用；

b) 其余比特置为 1 表示该证书支持对应的协议，一个证书可以支持多个协议；

c) AS 的根证书的强制域为“HUFU1”；

d) 二进制数 FLAG 的长度可扩展。

附 录 D
（资料性附录）
测试向量

D.1 SM2 测试向量

见 GM/T 0003—2012 附录 A 数字签名与验证示例。

D.2 SM3 测试向量

见 GM/T 0004—2012 附录 A 运算示例。

D.3 HMAC-SM3 测试向量

测试向量 1	
密钥	0x01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
密钥长度	32(八位位组)
数据	**abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopqabcdbcdecdefdefgefghfghighijhijkijkljkl mklmnlmnomnopnopq** 0x61 62 63 64 62 63 64 65 63 64 65 66 64 65 66 67 65 66 67 68 66 67 68 69 67 68 69 6a 68 69 6a 6b 69 6a 6b 6c 6a 6b 6c 6d 6b 6c 6d 6e 6c 6d 6e 6f 6d 6e 6f 70 6e 6f 70 71 61 62 63 64 62 63 64 65 63 64 65 66 64 65 66 67 65 66 67 68 66 67 68 69 67 68 69 6a 68 69 6a 6b 69 6a 6b 6c 6a 6b 6c 6d 6b 6c 6d 6e 6c 6d 6e 6f 6d 6e 6f 70 6e 6f 70 71
数据长度	112(八位位组)
消息鉴别码	0xca 05 e1 44 ed 05 d1 85 78 40 d1 f3 18 a4 a8 66 9e 55 9f c8 39 1f 41 44 85 bf df 7b b4 08 96 3

测试向量 2	
密钥	0x01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
密钥长度	37(八位位组)
数据	0xcd 重复 50 次
数据长度	50(八位位组)
消息鉴别码	0x22 0b f5 79 de d5 55 39 3f 01 59 f6 6c 99 87 78 22 a3 ec f6 10 d1 55 21 54 b4 1d 44 b9 4d b3 ae

测试向量 3	
密钥	0x0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b 0b
密钥长度	32(八位位组)
数据	**Hi There** 0x48 69 20 54 68 65 72 65
数据长度	8(八位位组)
消息鉴别码	0xc0 ba 18 c6 8b 90 c8 8b c0 7d e7 94 bf c7 d2 c8 d1 9e c3 1e d8 77 3b c2 b3 90 c9 60 4e 0b e1 1e

测试向量 4	
密钥	0x4a 65 66 65
密钥长度	4(八位位组)
数据	**what do ya want for nothing**? 0x77 68 61 74 20 64 6f 20 79 61 20 77 61 6e 74 20 66 6f 72 20 6e 6f 74 68 69 6e 67 3f
数据长度	28(八位位组)
消息鉴别码	0x2e 87 f1 d1 68 62 e6 d9 64 b5 0a 52 00 bf 2b 10 b7 64 fa a9 68 0a 29 6a 24 05 f2 4b ec 39 f8 82

D.4 KD-HMAC-SM3 测试向量

测试向量 1	
密钥	0x01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
密钥长度	32(八位位组)
数据	**pairwise key expansion for infrastructure unicast** 0x70 61 69 72 77 69 73 65 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 20 66 6f 72 20 69 6e 66 72 61 73 74 72 75 63 74 75 72 65 20 75 6e 69 63 61 73 74
数据长度	49(八位位组)
输出	0xb8 19 3a f1 bf f3 f6 db d9 ef 69 4e 73 dd e7 2a ab 5f b5 47 81 fe e2 8a 10 66 63 d8 42 c3 c5 27 5a 27 06 7f 94 68 18 75 25 cc 0c 5f 84 24 0e 8e
输出长度	48(八位位组)

测试向量 2	
密钥	0x01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
密钥长度	37(八位位组)
数据	**pairwise key expansion for infrastructure unicast** 0x70 61 69 72 77 69 73 65 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 20 66 6f 72 20 69 6e 66 72 61 73 74 72 75 63 74 75 72 65 20 75 6e 69 63 61 73 74
数据长度	49(八位位组)
输出	0x 6c c2 3e 56 f2 1b 03 6d fe 4a 49 a3 e9 fe c3 ee 6b bc 18 42 8a ac bf f5 11 8f 01 a1 65 8e 36 fb 2a 64 7b e1 b2 6e 41 72 3f 8e 24 2a c9 7f bc b3
输出长度	48(八位位组)

测试向量 3	
密钥	0x01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
密钥长度	16(八位位组)
数据	**pairwise key expansion for infrastructure unicast** 0x70 61 69 72 77 69 73 65 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 20 66 6f 72 20 69 6e 66 72 61 73 74 72 75 63 74 75 72 65 20 75 6e 69 63 61 73 74
数据长度	49(八位位组)
输出	0x04 a0 43 ce ee 28 3a 51 b2 b8 76 bc 9c 1c de 02 e9 c0 e8 b0 bf 12 cf ba cd 2b e4 f1 b4 50 61 41 87 f9 ff c1 bf 5f f9 da 62 b2 70 17 a5 59 ac 97
输出长度	48(八位位组)

测试向量 4	
密钥	0x01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
密钥长度	32(八位位组)
数据	**group key expansion for multicast and broadcast** 0x67 72 6f 75 70 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 20 66 6f 72 20 6d 75 6c 74 69 63 61 73 74 20 61 6e 64 20 62 72 6f 61 64 63 61 73 74
数据长度	47(八位位组)
输出	0x02 dd a4 62 2f 32 08 57 1e a8 e1 fe 2b db bf 1d 20 c2 00 0d 8f 60 08 94 a2 6f 4c 4f 59 4e 19 ce 31 fe 5c 1a d1 0e 60 af d2 b6 db 0e 42 b9 7b c0
输出长度	48(八位位组)

测试向量 5	
密钥	0x01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
密钥长度	37
数据	**group key expansion for multicast and broadcast** 0x67 72 6f 75 70 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 20 66 6f 72 20 6d 75 6c 74 69 63 61 73 74 20 61 6e 64 20 62 72 6f 61 64 63 61 73 74
数据长度	47
输出	0x82 f5 bf 8a c4 ea 8b 8a 88 c0 bd fb b9 f9 ee a4 d6 f4 c9 ef 82 66 44 83 2d fa 2a 16 e3 9c 0a dc 2d e2 a8 60 41 85 3f 58 84 b4 27 d4 e8 0e dd ee
输出长度	48

测试向量 6	
密钥	0x01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10
密钥长度	16
数据	**group key expansion for multicast and broadcast** 0x67 72 6f 75 70 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 20 66 6f 72 20 6d 75 6c 74 69 63 61 73 74 20 61 6e 64 20 62 72 6f 61 64 63 61 73 74
数据长度	47
输出	0xf3 37 69 c1 b6 b4 ad 18 6f cd d7 a5 32 b1 a0 b9 0f d0 ef f4 04 8a 84 59 9f 92 d7 00 dd 9f 81 b7 cb 01 8c a5 67 b7 59 11 6e 2f 27 d3 8f 11 b7 6c
输出长度	48

测试向量 7	
密钥	0x01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
密钥长度	32
数据	**pre-share key expansion for adhoc network** 0x70 72 65 2d 73 68 61 72 65 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 20 66 6f 72 20 61 64 68 6f 63 20 6e 65 74 77 6f 72 6b
数据长度	41
输出	0x8d d3 d8 4d af 0c b7 cf 65 9c 61 bb e8 66 46 ac 4c 74 67 d2 08 80 09 c1 8c 23 82 a6 9b 04 17 31 57 4b 9f a3 28 97 78 30 8d 78 54 40 04 b5 90 6a
输出长度	48

测试向量 8	
密钥	0x01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
密钥长度	37
数据	**pre-share key expansion for adhoc network** 0x70 72 65 2d 73 68 61 72 65 20 6b 65 79 20 65 78 70 61 6e 73 69 6f 6e 20 66 6f 72 20 61 64 68 6f 63 20 6e 65 74 77 6f 72 6b
数据长度	41
输出	0x19 87 c6 b4 1c 4b a4 b1 37 b0 5e 33 7d 19 90 ef 37 d9 da d5 66 c1 41 4f e9 e1 e8 0f c4 ae 6d 56 fc ba 61 b4 e5 3d b8 81 6c 13 2a 8d 6c 13 08 e7
输出长度	48

D.5 SM4-GCM 测试用例

加密：

参数名称	参数数据
Key(16 八位位组)	00 01 00 02 00 03 00 04 00 05 00 06 00 07 00 08
Iv(12 八位位组)	5c 36 5c 36 5c 36 5c 36 5c 36 5c 36
a(23 八位位组)	ff ff ff ff ff ff 00 03 7f ff ff fe 89 2c 38 00 00 5c 36 5c 36 5c 36
P(48 八位位组)	08 06 00 01 08 00 06 04 00 01 00 03 7f ff ff fe c0 a8 14 0a 00 00 00 00 00 00 c0 a8 14 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
输出 C(48 八位位组)	0a 59 91 a6 70 dc 0e a2 6f 84 e4 55 a1 c0 61 47 8a a0 9f 2f be 90 49 46 29 bc 58 e7 5b e5 e9 1d bc 6d 21 49 bc 1f ba ca ca a9 72 2d 61 0f de 1d
tag(16 八位位组)	99 20 b1 eb fb 59 02 5f 0e ba 77 8c f5 9a 5c c8

解密：

参数名称	参数数据
Key(16 八位位组)	00 01 00 02 00 03 00 04 00 05 00 06 00 07 00 08
Iv(12 八位位组)	5c 36 5c 36 5c 36 5c 36 5c 36 5c 36
a(23 八位位组)	ff ff ff ff ff ff 00 03 7f ff ff fe 89 2c 38 00 00 5c 36 5c 36 5c 36
P(48 八位位组)	0a 59 91 a6 70 dc 0e a2 6f 84 e4 55 a1 c0 61 47 8a a0 9f 2f be 90 49 46 29 bc 58 e7 5b e5 e9 1d bc 6d 21 49 bc 1f ba ca ca a9 72 2d 61 0f de 1d
输出 C(48 八位位组)	08 06 00 01 08 00 06 04 00 01 00 03 7f ff ff fe c0 a8 14 0a 00 00 00 00 00 00 c0 a8 14 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
tag(16 八位位组)	99 20 b1 eb fb 59 02 5f 0e ba 77 8c f5 9a 5c c8