国 际 电 信 联 盟

ITU-T X.1362

(03/2017)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

应用和服务的安全性 – 物联网（IoT）安全

物联网 (IoT) 环境的简单加密程序

ITU-T X.1362 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
PKI相关建议书	X.1340–X.1349
物联网（IoT）安全	**X.1360–X.1369**
智能交通系统（ITS）安全	X.1370–X.1379
网络安全信息交换	
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和导则	X.1640–X.1659
云计算安全的落实工作	X.1660–X.1679
其他云计算安全问题	X.1680–X.1699

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1362 建议书

物联网（IoT）环境的简单加密程序

摘要

人们认为，物联网（IoT）是未来最重要的标准化领域之一。从ITU-T的角度而言，IoT被定义为信息社会的全球性基础设施，通过（物理和虚拟）物体的互连促成先进业务。

在某些IoT环境中，特别是IoT设备方面，存在在一定时间段内对任务进行实时处理的需求。为确保数据保密性和完整性，最基本的对策之一即是采用数据加密/认证算法。数据加密/认证算法的标准应用存在的问题是无法满足上述要求。

ITU-T X.1362建议书规定物联网（IoT）设备的、带有相关掩膜数据的加密（EAMD）。本建议书具体阐明EADM以及该加密方法如何为使用它的流量提供一系列安全业务。

沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1362	2017-03-30	17	11.1002/1000/13196

关键词

数据加密/认证算法应用、带有掩膜数据的加密（EAMD）、物联网设备、物联网环境、实时处理要求。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

引言

人们认为，物联网（IoT）是未来最重要的标准化领域之一。从ITU-T的角度而言，[b-ITU-T Y.2060]将物联网定义为基于现有和不断演进的、可互操作信息通信技术的、信息社会的全球性基础设施，通过实现（物理和虚拟）物体的互连促成先进业务。

泛在传感器网络（USN）似乎是与物联网最为相关的领域之一。USN是智能传感节点网络，可“在任何时间、任何地点、由任何人和任何事物”加以部署。我们认为，泛在传感器网络（USN）的安全技术对物联网是有效的，因为从所处理的设备（如传感和驱动设备）角度而言，USN与物联网有众多相似之处。针对USN安全性，已发布了涉及安全框架的[b-ITU-T X.1311]、涉及中间件安全导则的[b-ITU-T X.1312]和涉及无线传感器网络路由安全要求的[b-ITU-T X.1313]。然而，迄今为止尚未出台为USN设备层提供安全的、有关数据保密性和完整性保护技术的建议书，因此，在USN和物联网方面，仍缺乏设备层安全规范。有鉴于此，应在未来对此做出讨论和研究并实现其标准化。

另一方面而言，在特定物联网环境中，特别是在物联网设备（如可用于工业控制系统（ICS）的传感和驱动设备）方面，存在在一定时间段内对任务进行实时处理的需求。为确保数据保密性和完整性，最基本的对策之一即是采用数据加密/认证算法。数据加密/认证算法的标准应用存在的问题是无法满足上述要求。另一个问题是对不同安全级别的综合：更具体而言，在通信数据包中，处于不同位置的数据需要有不同重要级别的安全性。因此，对低级别安全数据进行加密被认为是不必要的杂项开销。

如上所述，为实现物联环境的安全性，特别是物联网设备的安全性，需要形成对数据加密/认证算法的新应用，以满足实时处理要求并对不同安全级别予以综合。

有鉴于此，需要进行带有相关掩膜数据的加密，从而仅对通信数据包中安全级别高的数据进行加密。相关掩膜数据用来表明一个数据包中每一位置上数据的安全级别。

ITU-T X.1362 建议书

物联网（IoT）环境的简单加密程序

1 范围

本建议书提供物联网设备安全的加密程序。这一程序旨在用于物联网环境，特别是物联网设备，这些设备具有进行通信的强制功能以及进行感应、驱动、数据存储和数据处理的可选功能。本建议书规定物联网环境的带有相关掩膜数据（EAMD）的加密。本建议书具体阐明EAMD以及它如何为使用该加密手段的流量提供一系列安全业务。附件A还提供应用示例。

2 参考文献

下列ITU-T 建议书和其它参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其它参考文献均会得到修订，因此本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的ITU-T 建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[IETF RFC 4303] IETF RFC 4303 (2005)，IP封装安全有效载荷（ESP）。

[IETF RFC 7296] IETF RFC 7296 (2014)，互联网密钥交换协议版本2（IKEv2）

[IETF RFC 7321] IETF RFC 7321 (2014)，封装安全载荷（ESP）和认证字头（AH）的加密算法实施要求和使用指南

[ISO/IEC 10116] ISO/IEC 10116:2006，信息技术 – 安全方法 – n比特块密码的工作模式

3 定义

3.1 他处定义的术语

本建议书使用以下其它地方定义的术语：

3.1.1 激励器[ITU-T Y.4109]：在输入信号刺激后触发物理行动的设备。

注（自[ITU-T Y.2061]）– 举例而言，激励器可通过机械操作在气流或液体流或电流后产生行动。调光器和中继器都属于激励器。激活激励器的决定可能来自MOC应用、人或MOC设备和网关。

3.1.2 封装安全有效载荷（ESP）[IETF RFC 4303]：一种IPsec协议，用于提供保密性、数据来源认证、无连接完整性、抗重播业务（一种分数系列完整性形式）和（有限的）流量流动保密性。所提供的一系列业务取决于在建立安全关联（SA）时选择的选项，同时取决于在网络拓扑实施中的位置。

3.1.3 安全参数指数（SPI）[b-IETF RFC 4301]：一种任意的32位值，由接收方用来确定来向数据包应与之捆绑的SA。

3.1.4 传感数据[ITU-T F.4104]：由附加在某个传感器节点的传感器感知的数据。

3.1.5 传感器[ITU-T Y.4105]：传感物理条件或化合物并传递与所观测到的特性相关的电子信号的电子设备。

3.1.6 序号[IETF RFC 4303]：这一无符号的32位字段含一个计数器值，每发送一个数据包，值即加大，即，一个对应SA数据包的序号。

3.2 本建议书定义的术语

本建议书定义的术语如下：

3.2.1 可编程控制器：根据传感器发送的传感数据，对激励器进行控制的一种电子装置。

3.2.2 与掩膜相关的安全（SAM）：这是一套具体针对安全协议的参数。SAM通过采用带有相关掩膜数据的加密（EAMD）确定保护流量所需的业务和机制。SAM由其相关协议参引，取决于诸如传送层或互联网协议（IP）层的不同协议层。在这些参数中，可包括算法标识符、模式、和利用EAMD的层标识符及加密密钥。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

AES 先进加密标准

CBC 密码块链接

CMAC 基于密文的信息认证代码

EAMD 带有相关掩膜数据的加密

EAMDSP EAMD安全有效载荷

ESP 封装安全有效载荷

ICS 工业控制系统

IP 互联网协议

IPSec IP安全

IoT 物联网

IV 初始化矢量

MAC 信息认证代码

SA 安全关联

SAM 与掩膜相关的安全

SAMD SAM数据库

SPI 安全参数指数

TCP 传送控制协议

UDP 用户数据报协议

USN 泛在传感网

XOR 互斥或

5 惯例

无。

6 带有相关掩膜数据的加密（EAMD）介绍

6.1 EAMD程序规范

物联网环境面临众多安全威胁[b-ZT]。本建议书重点说明下列威胁：

1) 拦截合法数据或伪造合法数据、从而导致信息泄露或遭破坏的伪装攻击。

2) 窃听攻击 – 从网络上截获计算机发送的数据包并读取相关数据内容，以找到保密信息。

3) 欺骗攻击 – 伪装成合法成分，以获得数据或破坏信息。

为减缓物联网环境，特别是物联网设备的这些威胁，本建议书对带有相关掩膜数据的加密（EAMD）做出规范，该加密手段对一些设备间传送的明文通信数据包进行微小加密工作。加密工作包括加密/解密和信息认证代码（MAC）生成/认证及经认证的加密。EAMD采用的加密算法不属于本建议书的范围，但[b-ISO/IEC 9797]、[b-ISO/IEC 18033]和[b-ISO/IEC 19772]是加密算法、MAC算法和经认证加密算法的极好参考资料。

请注意，本节所述结构可视作使用加密–然后–MAC [b-ASIACRYPT]和[b-EUROCRYPT]的一种协议。

在通信数据包上，被实施加密操作的数据块用掩膜（mask）表示。

假设发送方了解EAMD安全通信的加密算法、密钥、初始矢量和掩膜，同时假设发送方和接收方相互间了解算法标识符和密钥。在这种条件下，通过在发送发一侧获得带有相关掩膜数据的加密信息而进行EAMD安全通信，同时与接收方共享加密信息。图1为带有相关掩膜数据的加密概览。

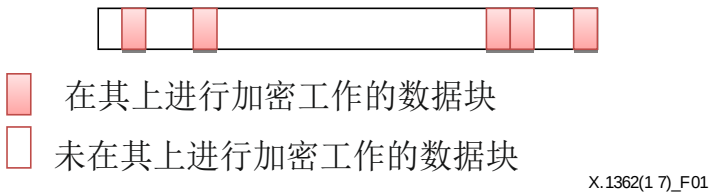


图1 – 使用带有相关掩膜数据加密的通信上传送的数据包

在EAMD安全通信中，去向处理程序如下：

1) 为加密增加必要填充（padding）。

2) 使用加密掩膜提取加密数据，并将其拷贝至进行临时计算的缓冲器中。

3) 利用密钥、加密算法和任何所需数据对缓冲器中的结果进行加密。

4) 利用掩膜将结果替换至数据包中。

5) 将结果封装至有效载荷字段。

如选择完整性，则处理如下：[1]

6) 利用生成MAC的掩膜提取生成MAC所需的数据，并将其拷贝至缓冲器中。

7) 为MAC生成增加必要填充。

8) 经缓冲器提供的结果生成MAC。

9) 将MAC增加到数据包中。

图2所示为去向处理程序。

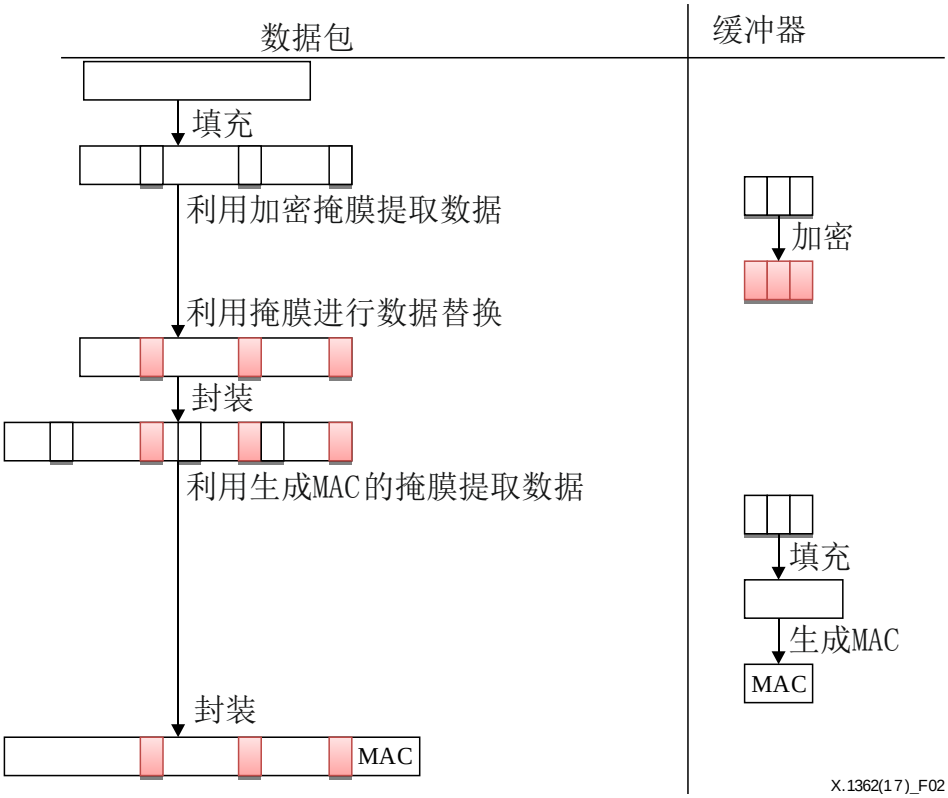


图2 – 在去向处理中利用带有相关掩膜数据的加密生成数据包

在EAMD安全通信中，来向处理程序如下：

如选择完整性，则进行下列1至3步骤：

1) 从数据包中提取数据，并按照生成MAC的掩膜，将MAC拷贝至缓冲器中。

2) 增加生成MAC所需的填充。

3) 利用已规定的完整性算法计算经过填充数据的MAC，并验证它是否与数据包中承载的MAC相同。如果计算和收到的MAC相吻合，则数据包有效，并被接受。如果验证失败，则接收方须将收到的数据包作为无效数据包丢弃。

4) 从数据包中移除字头。

5) 按照解密掩膜，将从结果中提取的数据存入缓冲器。

6) 在缓冲器中对提取结果解密。

---

1 要采用与IPsec协议绑定的带有相关掩膜数据的加密，应确保需经过验证的保密性。

7) 利用解密掩膜将缓冲器之中的结果替换至数据包。

8) 从数据包中移除加密填充。

图3具体说明来向处理程序。

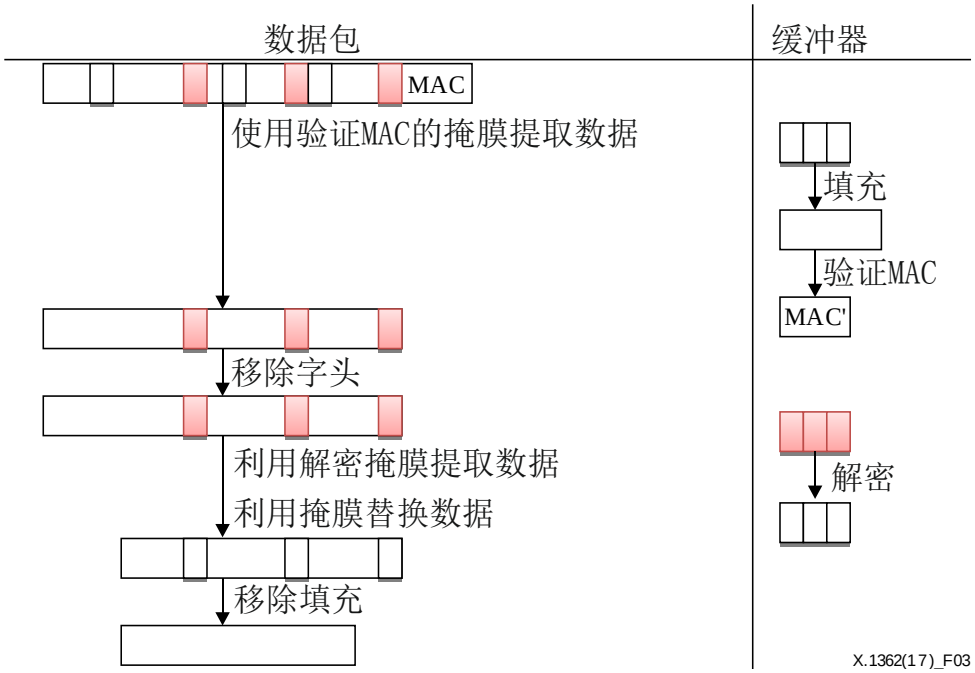


图3 – 在来向处理中利用带有相关掩膜数据的加密生成数据包

6.2 在带有掩膜数据的加密中进行目标数据提取的掩膜

在进行带有相关掩膜数据的加密工作时，通过将数据包分裂为块尺寸（根据掩膜参数使用加密算法）来提取输入到相应算法中的目标数据块。

7 带有相关掩膜数据的加密

本节阐述如何在每一层为流量提供一系列安全业务。本建议书描述使用带有相关掩膜数据的加密（以EAMD安全有效载荷（EAMDSP）为基础）的安全通信。图4概要说明这种通信。以下阐明EAMD安全通信的详细流程：

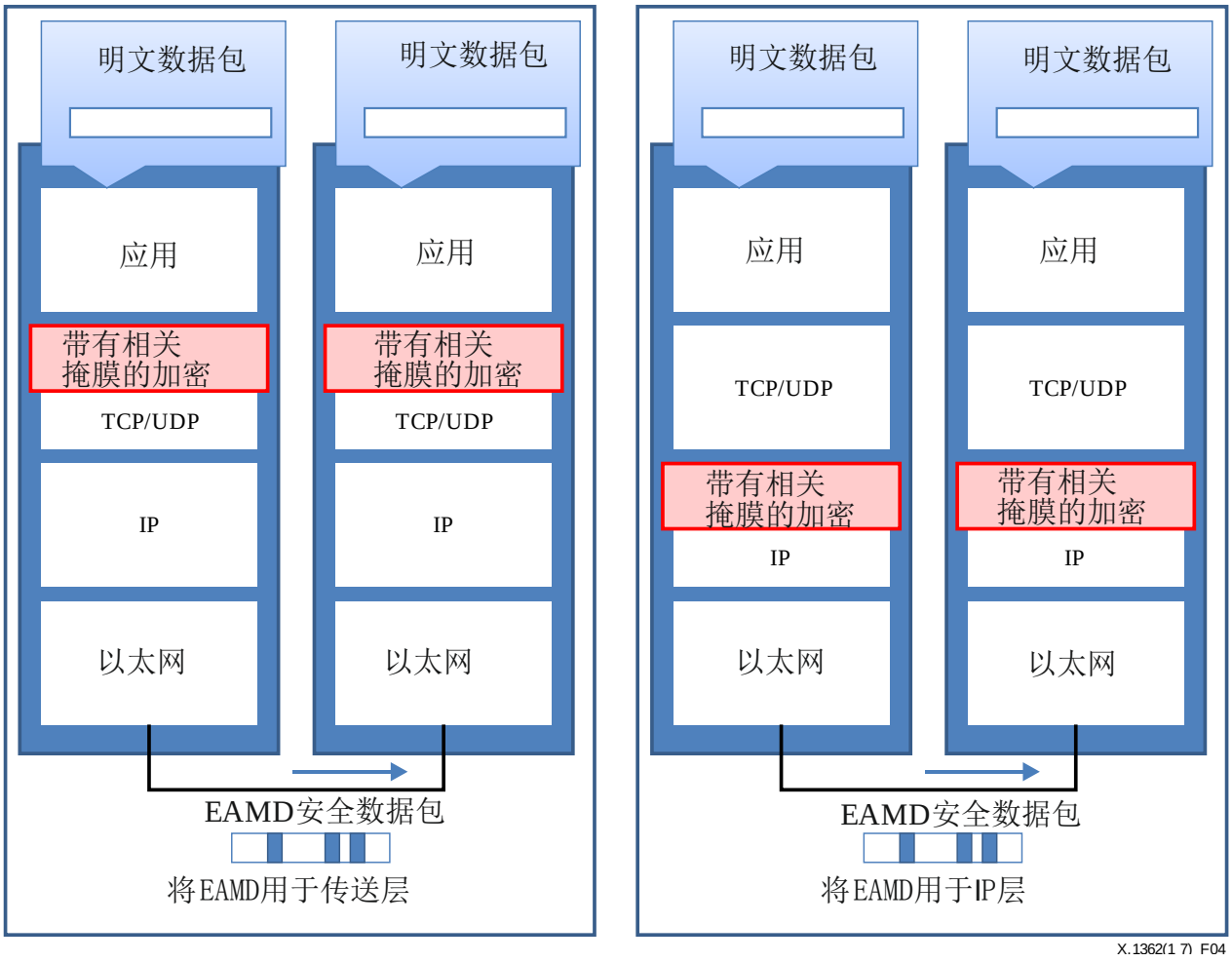


图4 – 使用带有相关掩膜数据的加密（EAMD）的通信概览

7.1 与掩膜相关的安全（SAM）

与掩膜相关的安全（SAM）被定义为一套针对具体安全协议的参数。SAM确定保护使用EAMD流量所需的业务和机制。SAM由其相关协议参引，取决于诸如传送层或互联网协议（IP）层的协议层。在这些参数中，可包含采用EAMD的算法标识符、模式、层标识符以及针对具体层的参数，如IP地址和端口及加密秘钥。SAM包含被定义为一套加密参数的CryptCtx。在SAM数据库（SAMD）中亦呈现与SAM相关的状态数据。

表1给出此格式中的每一个强制性参数。

表1 – 安全关联（SA）中CryptCtx的强制性参数

编号	参数	含义
1	encAlg	加密算法标识符
2	encKey	加密秘钥
3	encMask	被加密的区

表2给出各可选参数。

表2 – SA中CryptCtx的可选参数

编号	参数	含义
1	encRoundKey	加密回合秘钥
2	decRoundKey	解密回合秘钥
3	encIV	加密初始矢量（IV）
4	macRoundKey	MAC回合秘钥
5	macK1	CMAC K1子秘钥
6	macK2	CMAC K2子秘钥
7	KeyStream	事先生成的任意号码
8	KeyStreamHead	指向未使用任意号码字首的指针
9	KeyStreamTail	指向未使用任意号码尾端的指针
10	EncIVTail	任意号码生成初始矢量
11	macAlg	MAC算法标识符
12	macKey	MAC秘钥
13	macMask	用以通过指定算法生成MAC的区域

7.2 EAMD安全有效载荷（EAMDSP）的数据包格式

图5具体说明EAMD安全有效载荷（EAMDSP）数据包的格式。该数据包以长度可变的EAMDSP字头开始，此字段后为有效载荷数据，其子结构取决于所选择的加密算法和模式。有效载荷数据之后是填充和填充长度字段，然后为下一个字头字段，数据包的结尾处是可选的信息认证代码（MAC）字段。EAMDSP的拖尾（trailer）由填充、填充长度和下一个字头字段组成。

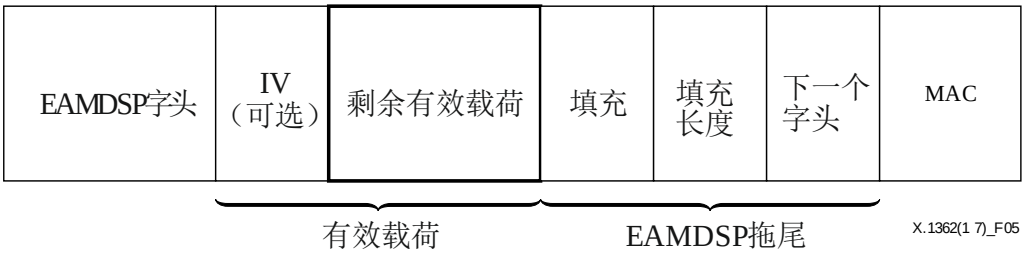


图5 – EAMDSP数据包格式

（被发送）EAMDSP拖尾由填充、填充长度和下一个字头字段组成。在完整性计算中，包含更多的隐性EAMDSP拖尾数据（不传送）。

如选择完整性业务，则完整性计算包括EAMDSP字头、有效载荷数据和EAMDSP拖尾。如果选择保密性业务，则密码文本由有效载荷数据（可能被包含在内的任何加密同步数据除外）和EAMDSP拖尾组成。

以下各节阐明字头格式中的字段。“可选”表示，如果未选择该选项，则省略相应字段，即，在计算MAC中，该字段即不包含在被传送的数据包中，也不被包含在被格式化的数据包中。是否选择某一选项是作为与掩膜相关安全（SAM）建立工作的一部分确定的，因此，在SAM的整个过程中，特定SAM的EAMDSP数据包格式是固定的。与之相反，“强制性”字段总是出现在所有SAM的EAMDSP数据包格式中。

7.2.1 有效载荷数据

有效载荷数据是长度可变的字段，包含由下一个字头字段描述的（来自最初数据包）的数据。有效载荷数据字段是强制性的，其长度呈整数字节。如果有效载荷加密所用算法要求使用加密同步数据，如初始化矢量（IV），那么该数据在有效载荷字段中显性承载，但在EAMDSP中不作为单独字段凸显，即，对EAMDSP而言，显性IV的传送是看不见的。

7.2.2 填充（用于加密）

如果所用加密算法要求的明文（plaintext）为数个若干字节，如，密文块的块尺寸，则采用填充字段将明文（由有效载荷数据、填充、填充长度和下一个字头字段组成）填充至算法所需尺寸。

7.2.3 填充长度

填充长度字段表明在填充字段中紧靠填充前的填充字节数。填充长度字段是强制性的。

7.2.4 下一个字头

下一个字头是强制性的。该字段明确有效载荷数据字段所含数据的类别，如，下一层字头和数据。

7.2.5 信息认证代码（MAC）

信息认证代码是一个长度可变字段，经过掩膜所示的在完整性方面需予以保护的数据计算得出。隐性EAMDSP拖尾字段（如生成MAC的填充）被包含在MAC计算之中。MAC字段是可选字段，仅在选择完整性业务时出现，且会通过单独的完整性算法或通过使用MAC的混合式算法提供。该字段的长度由选定的与SAM相关的算法确定。完整性算法规范须规定MAC长度以及进行验证的比较规则和处理步骤。

7.3 数据包处理

7.3.1 去向数据包处理

利用带有相关掩膜数据的加密的去向处理程序如下：

1) SAM查找：

将EAMDSP用于去向数据包前，需根据一些信息，如数据包中的层标识符和具体针对层的参数（如IP地址或端口号码），确定需要进行EAMDSP处理的相关SAM。SAM表明加密和生成MAC的密钥和掩膜。

2) 第6.1节阐述如何利用EAMD进行数据转换。

3) 数据包发送：

将最初字头加到经EAMD转换的数据包中并将最终形成的数据包发送到网络。

7.3.2 来向数据包处理

利用带有相关掩膜数据的加密的来向处理程序如下：

1) SAM查找：

一旦收到含有EAMDSP字头的数据包，则接收方通过SAMD中的查表确定适当的SAM。SAM的SAMD条目亦表明在去向处理过程中在哪一层采用EAMD、数据包中与层相关的参数（如IP地址或端口编号）以及MAC字段是否应当出现。此外，SAMD条目还规定解密和MAC验证（如适用的话）所采用的算法和密钥。

2) EAMDSP字头数据验证：

可采用EAMDSP字头中的特定数值对EAMDSP字头数据进行检查并在完整性检查和解密之前完成。如果数据包未通过这一检查，则被丢弃。

第6.1节阐明如何利用EAMD进行数据转换。

8 使用经认证的加密算法的EAMD

8.1 与掩膜相关的安全（SAM）

对于采用认证加密算法的EAMD，第7.1节也定义了与掩膜相关的安全（SAM）。

表3阐明本格式中的每一项强制性参数。

表3 – SA中CryptCtx的强制性参数

编号	参数	含义
1	auencAlg	经认证的加密算法标识符
2	auencKey	经认证的加密密钥
3	encMask	正在加密的区域

表4阐明各项可选参数。

表4 – SA中CryptCtx的可选参数

编号	参数	含义
1	auencRoundKey	经认证的加密回合密钥
2	audecRoundKey	解密回合密钥
3	IV	经认证的加密初始矢量
4	Nonce	经认证的加密回合密钥

8.2 EAMD安全有效载荷（EAMDSP）的数据包格式

图6具体表明EAMDSP（EAMD安全有效载荷）数据包的格式。数据包以长度可变的EAMDSP字头开始，该字段后为有效载荷数据（其子结构取决于所选的加密算法和模式）。有效载荷数据后为填充和填充长度字段以及下一个字头字段。EAMDSP拖尾由填充、填充长度和下一个字头字段组成。

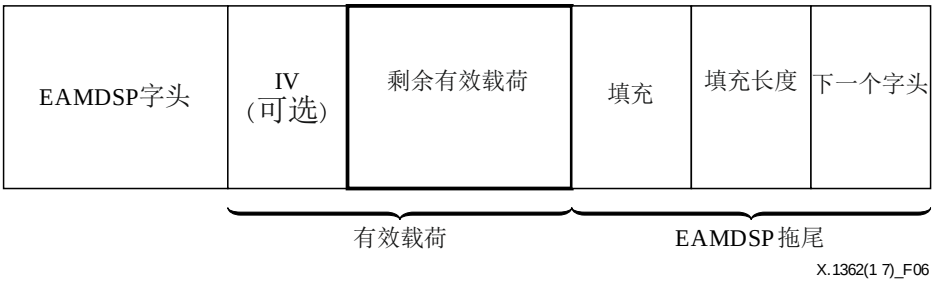


图6 – 无MAC的EAMDSP（用于经认证的加密）数据包格式

（被传送的）EAMDSP拖尾由填充、填充长度和下一个字头字段组成。在完整性计算中还包含更多的隐性EAMDSP拖尾数据（不传送）。

如选择完整性业务，则完整性计算包含EAMDSP字头、有效载荷数据和EAMDSP拖尾。如选择保密性业务，则密文由有效载荷数据（可能包含的任何加密同步数据除外）和EAMDSP拖尾组成。

以下各节阐述字头格式的字段。“可选”的含义是，如果未选择该可选功能，则该字段可省去，即，该字段既不出现在被传送的数据包中，也不出现在计算MAC的格式中。是否选择某一可选功能是作为与掩膜相关的安全（SAM）建立工作的一部分确定的，因此，在SAM过程中，特定SAM的EAMDSP数据包格式是固定的。与此相反，“强制性”字段总是出现在所有SAM的EAMDSP数据包格式中。

8.2.1 有效载荷数据

有效载荷数据是一个长度可变的字段，包含由下一个字头字段描述（来自最初数据包）的数据。有效载荷数据字段是强制性的，其长度为呈整数字节。

封装安全载荷（ESP）数据包的格式可表述为ESP = SPI ||序号|| IV || C，其中C是经认证的加密算法产生的密文。在此情况下，C纳入了认证标签。

8.2.2 填充（用于经认证的加密）

如果所用经认证的加密算法要求的明文为数个若干字节，如，密文块的块尺寸，则采用填充字段将明文（由有效载荷数据、填充、填充长度和下一个字头字段组成）填充至算法所需尺寸。

8.2.3 填充长度

填充长度字段表明填充字段中紧靠填充前的填充字节数。填充长度字段是强制性的。

8.2.4 下一个字头

下一个字头是强制性字段。该字段明确有效载荷数据字段所含的数据类别，如下一层字头和数据。

8.3 数据包处理

8.3.1 去向数据包处理

采用带有相关掩膜数据的加密的来向处理程序如下：

1) SAM查找：

在将EAMDSP用于去向数据包之前，根据一些信息，如层标识符和数据包中具体针对层的参数（如互联网协议（IP）地址或端口号码），确定要进行EAMDSP处理的相关SAM。SAM表明经认证的加密的密钥和掩膜。

2) 采用EAMD经认证加密模式的数据转换

1) 为加密增加必要的填充。

2) 利用加密掩膜提取加密数据，并将其拷贝至用作进行临时计算的缓冲器中。

3) 在缓冲器中用密钥、加密算法和任何所需的数据对结果进行加密。

4) 利用掩膜将加密文本替换至数据包中。

5) 将认证标签作为MAC加至数据包。

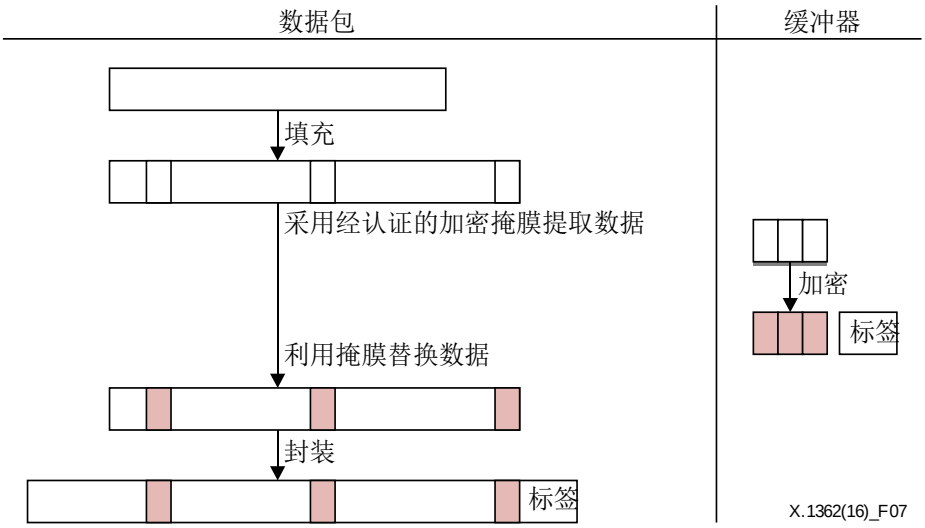


图7 – 经认证的加密模式的去向数据包处理

3) 数据包发送：

最初字头被增加到经EAMD转换的数据包中，并将最终数据包发至网络。

8.3.2 来向数据包处理

采用带有相关掩膜数据的加密的来向处理程序如下：

1) SAM查找：

接收方一旦收到含有EAMDSP字头的数据包，则通过SAMD查表确定适当的SAM。用于SAM的SAMD条目亦表明在去向处理过程中在哪一层使用了EAMD以及数据包中与层具体相关的参数（如IP地址或端口号码）。此外，SAMD条目还确定进行解密和标签验证将使用的算法和密钥。

2) EAMDSP字头数据验证：

可采用EAMDSP字头中的特定数值对EAMDSP字头数据进行检查并在完整性检查和解密之前完成。如果数据包未通过这一检查，则被丢弃。

3) 采用EAMD经认证解密模式的数据转换

1) 从数据包中去除字头。

2) 利用解密掩膜提取解密数据，并将其拷贝至用于临时计算的缓冲器中。

3) 从数据包中分离认证标签并将其拷贝至缓冲器。

4) 利用密钥、解密算法和任何所需数据在缓冲器中对结果进行解密。

5) 如果解密成功，则利用掩膜将解密结果替换至数据包中。

4) 从数据包中去除加密填充。

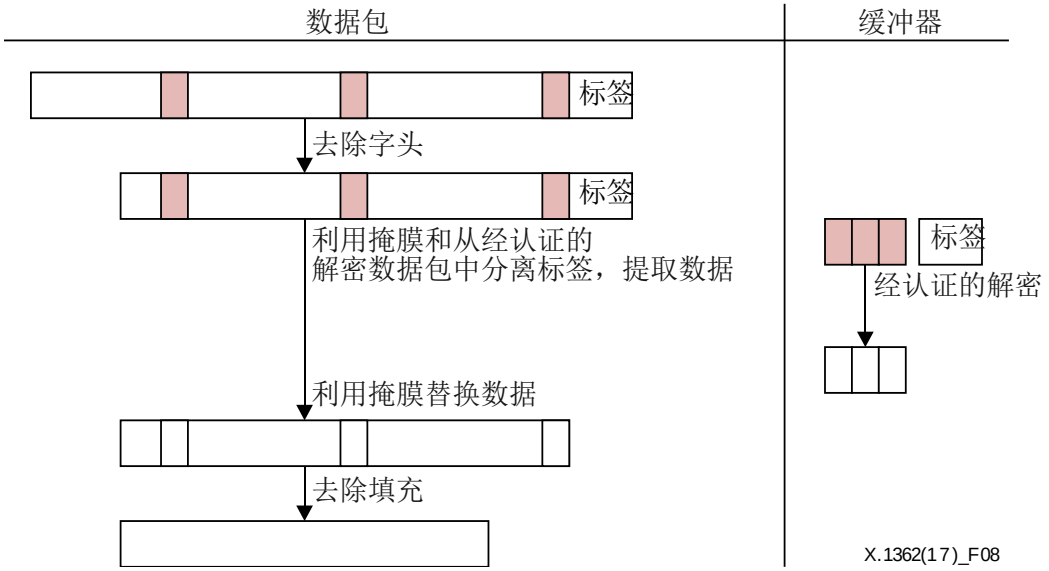


图8 – 经认证的加密模式的来向数据包处理

9 指南和限制

9.1 有关建立SAM的指南

在EAMD加密掩膜方法方面，应当指出，如果恶意实体能够修改掩膜，则他们可以将掩膜数值设定为任何数据都无法得到加密的程度。一旦掩膜被这样修改，则设备的所有数据都将“畅行无阻”（即，得不到加密）地被沟通。这将是一种十分重大的安全漏洞。

为解决这一问题，应研究解决下列问题：

1) 掩膜通信安全

为了实现加密材料（如加密密钥、初始矢量和其他安全参数）的初始化和对其进行更新，需采用一些密钥建立协议，如互联网密钥交换协议版本2（IKEv2）[IETF RFC 7296]、密钥协议和密钥传送。

应确保通过利用这些协议在相关实体进行通信过程中，针对密钥材料的初始化和更新来确保掩膜被初始化和更新。例如，在密钥建立通信过程中，上述密钥资料也应包含掩膜，以便通过这些协议中使用的加密算法和MAC算法实现掩膜的完整性和保密性。

2) 掩膜存储安全

应确保一旦掩膜处于设备上，则不存在任何其他设备可识读掩膜的协议。

建议采用下列方法实现这一目的。

第一种方法是进行安全的系统设计，在分配系统成分时，采用EAMD的设备不直接与系统外实体通信，但有很高计算能力的安全网关成分与实体通信。

第二个方法是通过抗破坏硬件或软件迷乱 – 后者创建一种人们难以明白的模糊代码 – 来保护设备。

9.2 关于适当使用初始化矢量和特定场合（nonce）的指南

本节阐明适当使用初始化矢量（以及更多块密文模式和填充）的指南。对初始化矢量或填充使用不当往往会造成陷阱，使协议受到攻击。IV或特定场合很可能在协议安全性方面发挥至关重要的作用。

为了在加密中使用密码块链接（CBC）模式[ISO/IEC 10116]（其特点是将明文块与此前的密文块相结合），应采取下列行动：

如果将CBC模式用作密文块操作模式，则应考虑针对[b-CBCPADD]中所述填充甲骨文（padding oracle）攻击。CBC模式要求IV与首个明文块结合。IV不一定需要是秘密的，但必须是不可预测的。

为了安全使用经认证的加密算法，应采取下列行动：

如应用不能满足特定场合生成的独特性要求，那么则须使用零长度特定场合。任意化的或状态化的算法[b-IETF RFC 5116]适用于这类应用。如若不然，应用应使用具有十二个八字节长度的特定场合。

当特定场合或IV得到重复时，许多遭到实际攻击的方案将会显露出两个数据包的互斥或（XOR），因此，强烈推荐保证IV或特定场合是独一无二的。

9.3 使用EAMD的限制

在系统实时性能要求中，EAMD的使用是有限制的。

EAMD是在发送方和接收方都拥有一定程度计算能力（如CPU架构为16比或32比，并带有合理频率（数百MHz）和内存）时，在系统中最优。

应当指出，如果系统有功率限制要求，则EAMD可能不是一种好的解决方案，因为EAMD缓存处理的功耗可能带来大量杂项开销。

还应当指出，如上所述，掩膜如同加密密钥一样，非常敏感，因此只有在设想掩膜可以得到安全管理和保护的情况下，才可以使用EAMD。

附件A

与现有协议的绑定

（本附件构成本建议书不可分割的部分）

对于采用带有相关掩膜数据的加密安全通信，加密层须固定。可在多个可能的层进行这种行动，如选择传送层和IP层等。本附件阐述如何将带有相关掩膜数据的加密与现有协议进行绑定。相关掩膜数据与IPsec协议绑定的使用需实现保密和认证。应确保通过认证实现保密[IETF RFC 7321]。

A.1 与IP安全（IPSec）ESP协议IETF RFC 4303的绑定

A.1.1 SAM格式

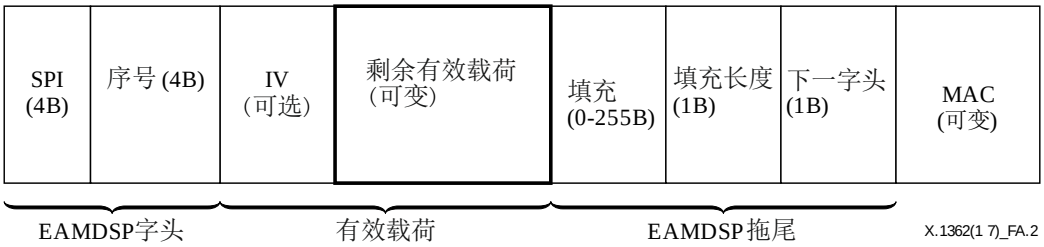
SAM确定对采用EAMD流量予以保护的必要业务和机制。如果将EAMD用于网络层，则与掩膜相关的安全（SAM）的格式为图A.1所示格式。

```
SecurityAssertion ::= SEQUENCE {
  layerIdentifier OCTET STRING (SIZE(1)),
  SPI             OCTET STRING (SIZE (4)),
  ipAddr          OCTET STRING (SIZE (4)),
  cryptCtx        CryptCtx
}
CryptCtx ::= SEQUENCE {
  encAlg    OCTET STRING (SIZE (4))
  encKey    OCTET STRING (SIZE (keySizeMax)),
  encMask   OCTET STRING (SIZE (maskLength))
}
keySizeMax INTEGER ::= 64
maskLength INTEGER ::= 16
```

图A.1 – 网络层的SAM格式

A.1.2 数据包格式

图A.2以示例表明EAMD安全有效载荷（EAMDSP）数据包的格式。该数据包以长度可变的EAMDSP字头开始，该字段后是有效载荷数据，其子结构取决于所选的加密算法和模式。有效载荷数据之后是填充和填充长度字段，再之后为下一个字头字段。数据包的结尾处为可选信息认证代码（MAC）字段。EAMDSP拖尾由填充、填充长度和下一个字头字段组成。考虑到由于EAMD MAC计算和EAMD加密带来的流量数量，因此在另一个格式示例中，显示了8B的序号长度和在EAMDSP字头中放入的下一个字头字段。



图A.2 – 与IPSec ESP协议绑定的EAMDSP数据包格式示例

1) 安全参数指数（SPI）：

SPI是一个32位的任意数值，可由接收方用来确定数据包与之绑定的SAM。SPI字段是强制性的。SPI在协议中得到承载是为了使接收系统选择将在其之下处理所收到数据包的SAM。

2) 序号：

该没有符号的32位或64位字段包含一个计数器值，每发送一个数据包值增加一，即，对应每一SAM数据包的序号，或其替代方法是，按照清晰明了规则产生一个数值。

3) 有效载荷数据：

有效载荷数据是长度可变的、含有由下一个字头字段描述数据（来自最初数据包）的字段。有效载荷数据字段是强制性的，长度呈整数字节。如果有效载荷加密使用的算法需要加密同步数据，如，初始化矢量（IV），则该数据在有效载荷字段中显性承载，但不在EAMDSP中作为单独字段被调出。即，显性IV传送对EAMDSP是不可见的。

4) 填充（用于加密）：

不论加密算法要求如何，都需要有填充，以确保最终得出的密文终止在4字界线上。具体而言，填充长度和下一个字头字段须与4字节字完全对应（正如关于EAMDSP数据包格式的上图所示），以确保MAC字段（如存在的话）在4字节界线上。

5) 填充长度：

填充长度字段表明填充长度字段中紧靠其前面的填充字节的数量。有效数值范围为0到255，其中0表示不存在填充字节。填充长度字段是强制性的。

6) 下一个字头：

下一个字头是一个强制性的8位字段，明确有效载荷数据字段所含数据的类别，如下一层字头和数据。

7) 信息认证代码（MAC）：

信息认证代码是长度可变的字段，经掩膜表明需保护完整性的数据计算。隐形EAMDSP拖尾字段，如生成MAC的填充，包含在MAC计算中。MAC字段是可选的。

A.1.3 数据包处理

使用带有相关掩膜数据的加密的去向处理程序如下：

1) SAM查找：

需要进行EAMDSP处理的相关SAM是根据下列信息确定的：层标识符和与层具体相关的参数，如数据包中的IP地址或端口号码。

2) 使用EAMD的数据转换：

按照第6.1节所述程序利用EAMD进行加密并生成MAC。

3) 数据包发送：

将最初字头加到经EAMD转换的数据包中并将最终形成的数据包发送至网络。

使用带有相关掩膜数据的加密的来向处理程序如下：

1) SAM查找：

需要进行EAMDSP处理的相关SAM是根据下列信息确定的：层标识符和与层具体相关的参数，如数据包中的IP地址或端口号码。

2) 序号验证：

通过使用EAMDSP字头中序号值检查序号并在完整性检查和解密前进行。如果未通过检查，则数据包被丢弃。

3) 使用EAMD进行数据转换：

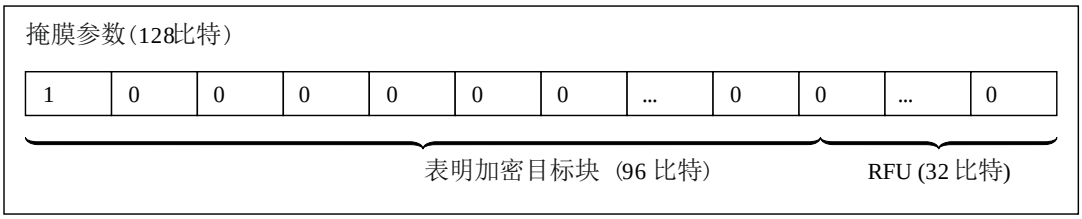
根据第6.1节所述程序利用EAMD进行MAC验证和解密。

A.1.4 带有相关掩膜数据的加密的目标数据提取掩膜

在进行带有相关掩膜数据的加密时，通过按照掩膜参数将数据包分离为所使用加密算法的块尺寸，提取输入到相应算法中的目标块。例如，在使用先进加密标准（AES）的带有相关掩膜数据的加密时，有效载荷被分离为128比特的块，因为AES的块长度为128比特。通过按照掩膜发现相关块，可提取目标解密块。之后，将目标解密块进行串联，以生成操作所需的目标数据。图A.3和A.4表明掩膜格式。这一参数表明，如果将有效载荷分离为所使用加密算法的块尺寸，则应对哪些块进行加密或解密。

```
MaskFormat ::= SEQUENCE {
  encryptionArea OCTET STRING (SIZE (12))
  reserved OCTET STRING (SIZE (4))
}
```

图A.3 – 掩膜格式



图A.4 – 掩膜参数详细格式

在这种情况下，该掩膜参数的含义是，只有第一个块得到加密，因为该掩膜参数的第一位是真实的。一些区的加密要求将掩膜参数的某些位由虚假变为真实。

A.1.5 填充算法

可将填充算法描述如下：

– 在有效载荷结尾处附上一个'0x80'。

– 如果有效载荷的长度是多个加密算法块长度，则填充完成。

如果有效载荷长度并非是多个加密算法块长度，则在有效载荷结尾处附上'0x00'，直到有效载荷的长度为多个块长度。

参考资料

[b-ITU-T F.4104] Recommendation ITU-T F.4104/F.744 (2009), *Service description and requirements for ubiquitous sensor network middleware.*

[b-ITU-T X.1311] Recommendation ITU-T X.1311 (2011) | ISO/IEC 29180:2012, *Information technology – Security framework for ubiquitous sensor networks.*

[b-ITU-T X.1312] Recommendation ITU-T X.1312 (2011), *Ubiquitous sensor network middleware security guidelines.*

[b-ITU-T X.1313] Recommendation ITU-T X.1313 (2012), *Security requirements for wireless sensor network routing*.

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ITU-T Y.4105] Recommendation ITU-T Y.4105/Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment.*

[b-ITU-T Y.4109] Recommendation ITU-T Y.4109/Y.2061 (2012), *Requirements for the support of machine-oriented communication applications in the next generation network environment.*

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol.*

[b-IETF RFC 5116] IETF RFC 5116 (2008), *An Interface and Algorithms for Authenticated Encryption.*

[b-ISO/IEC 9797] ISO/IEC 9797-1:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher.*

[b-ISO/IEC 18033] ISO/IEC 18033-3:2010, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.*

[b-ISO/IEC 19772] ISO/IEC 19772:2009, *Information technology – Security techniques – Authenticated encryption.*

[b-ASIACRYPT] Bellare, M., and Namprempre, C. (2000), *Authenticated encryption:* Relations *among notions and analysis of the generic composition paradigm*, in Tatsuaki Okamoto, editor, ASIACRYPT 2000, Vol. 1976 of LNCS, Springer, December, pp. 531-545.

[b-CBCPADD] Vaudenay, S. (2002), *Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS*, EUROCRYPT 2002.

[b-EUROCRYPT] Namprempre, C., Rogaway, P., and Shrimpton, T. (2014), *Reconsidering generic composition*, in Phong Q. Nguyen and Elisabeth Oswald, editors, EUROCRYPT 2014, Vol. 8441 of LNCS, Springer, May, pp. 257-274.

[b-ZT] Li, Zhang, and Xin, Tong (2013), *Threat Modeling and Countermeasures Study for the Internet of Things*, Journal of Convergence Information Technology (JCIT), Vol. 8, No. 5, March.

ITU-T 系列建议书

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2018年，日内瓦