

# 中华人民共和国国家标准

GB/T 43844—2024

## IPv6 地址分配和编码规则 接口标识符

IPv6 address assignment and coding rules—Interface identifier

2024-04-25发布

2024-11-01 实施

国家市场监督管理总局  
国家标准化管理委员会

发布



目 次

前言 ..... III

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 2

5 IPv 6全球单播地址格式 ..... 2

6 接口标识符编码方法 ..... 2

    6.1 EUI -64 编码方法 ..... 2

    6.2 加密变换编码方法 ..... 3

附录 A(资料性) 加密变换编码方法计算实例 ..... 4

参考文献 ..... 6



# 前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)和全国通信标准化技术委员会(SAC/TC 485)归口。

本文件起草单位：国家计算机网络应急技术处理协调中心、清华大学、四川大学、华为技术有限公司、中兴通讯股份有限公司、中国信息通信科技集团有限公司、华东师范大学、北京百度网讯科技有限公司、奇安信网神信息技术(北京)股份有限公司、北京中关村实验室。

本文件主要起草人：陈训逊、王文磊、崔牧凡、李高超、刘莹、何林、陈兴蜀、曾雪梅、肖佃艳、周继华、王晖、周箴、王璇、陈恺、郭建领、邹昕、张伟、李祥学、施新刚、吴萍、安锦程、孙杰。



# IPv6地址分配和编码规则 接口标识符

## 1 范围

本文件规定了IPv6 地址接口标识符的编码规则。

本文件适用于互联网接入服务商、应用基础设施服务商、自用网络运营者、网络终端厂商、网络设备厂商等进行网络动态分配IPv6 地址时的接口标识符编码与分配。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 25069—2022 信息安全技术 术语

## 3 术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

### 3.1

**接口标识符 interface identifier;IID**

在一条链路上，用于标识网络内特定接口的标识符(IPv6 地址中的低比特部分)。

### 3.2

**互联网接入服务商 internet access service provider**

拥有全国性或区域性用户接入网络，为终端用户提供专线、拨号上网等接入互联网的服务及有限的信息服务的提供商。

### 3.3

**应用基础设施服务商 application infrastructure provider**

提供全国性和区域性的互联网数据中心服务、云计算服务、内容分发网络服务、域名注册和解析服务的服务提供商。

### 3.4

**自用网络 self-operating network**

除互联网接入服务商和应用基础设施服务商之外，从境内地址分配机构获得地址或从亚太互联网信息中心等具有IP 地址管理权的国际机构获得地址的网络。

### 3.5

**网络终端 network terminal**

一种具有网络功能接入能实现人与机器交互的终端设备。

[来源：GB/T 36465—2018]

### 3.6

**IPv6动态主机配置协议 dynamic host configuration protocol for IPv6;DHCPv6**

一种动态配置协议，用于配置IPv6 节点的网络配置参数、IPv6 地址以及 IPv6 地址前缀的可扩展

机制。  
[来源：IETF RFC 8415]

3.7

无状态地址自动配置 stateless address autoconfiguration;SLAAC

由节点生成接口标识符，并与节点通过监听路由通告获得的地址前缀结合形成IPv6 地址的一种动态配置协议。

4 缩略语

- 下列缩略语适用于本文件。
- EUI-64:64 位扩展唯一标识符(64-bit Extended Unique Identifier)
- IETF: 国际互联网工程任务组(Internet Engineering Task Force)
- IMEI: 国际移动设备识别码(International Mobile Equipment Identity)
- IPv6: 互联网协议第6版(Internet Protocol Version 6)
- MAC: 媒体访问控制(Media Access Control)
- MSB:最高有效位(Most Significant Bit)
- RFC: 请求评议文件(Request for Comments documents)

5 IPv6 全球单播地址格式

IPv6 地址长度为128位，除了以二进制000开始的全球单播地址外，IPv6 全球单播地址的接口标识符长度均为64位。IPv6 全球单播地址一般格式见图1。

n位-		(64—n) 位-	64位-
路由前缀		子网标识符	接口标识符

图 1 IPv6 全球单播地址格式

接口标识符编码方法见第6章。

6 接口标识符编码方法

6.1 EUI-64 编码方法

该编码方法采用IETF RFC 4291的附录A, 适用于互联网接入服务商、应用基础设施服务商、自用网络运营者等IPv6 地址运营实体通过DHCPv6 向网络终端分配IPv6 地址时的接口标识符编码，也适用于通过SLAAC 由网络终端生成的接口标识符编码。编码方法如下(见图2)：

- a) 在 MAC 地址的制造商标识符和网络适配器标识符之间插入 “0xff”和“0xfe”作为中间16位；
- b) 对 a) 形成的64位的自左向右第7位进行取反操作(接口标识符第7位用于标识该接口标识符是全局唯一或本地唯一。0表示该接口标识符本地唯一，1表示该接口标识符全局唯一), 生成的64位即为接口标识符。

注：MAC地址共48位，前24位为制造商标识符，后24位为网络适配器标识符。



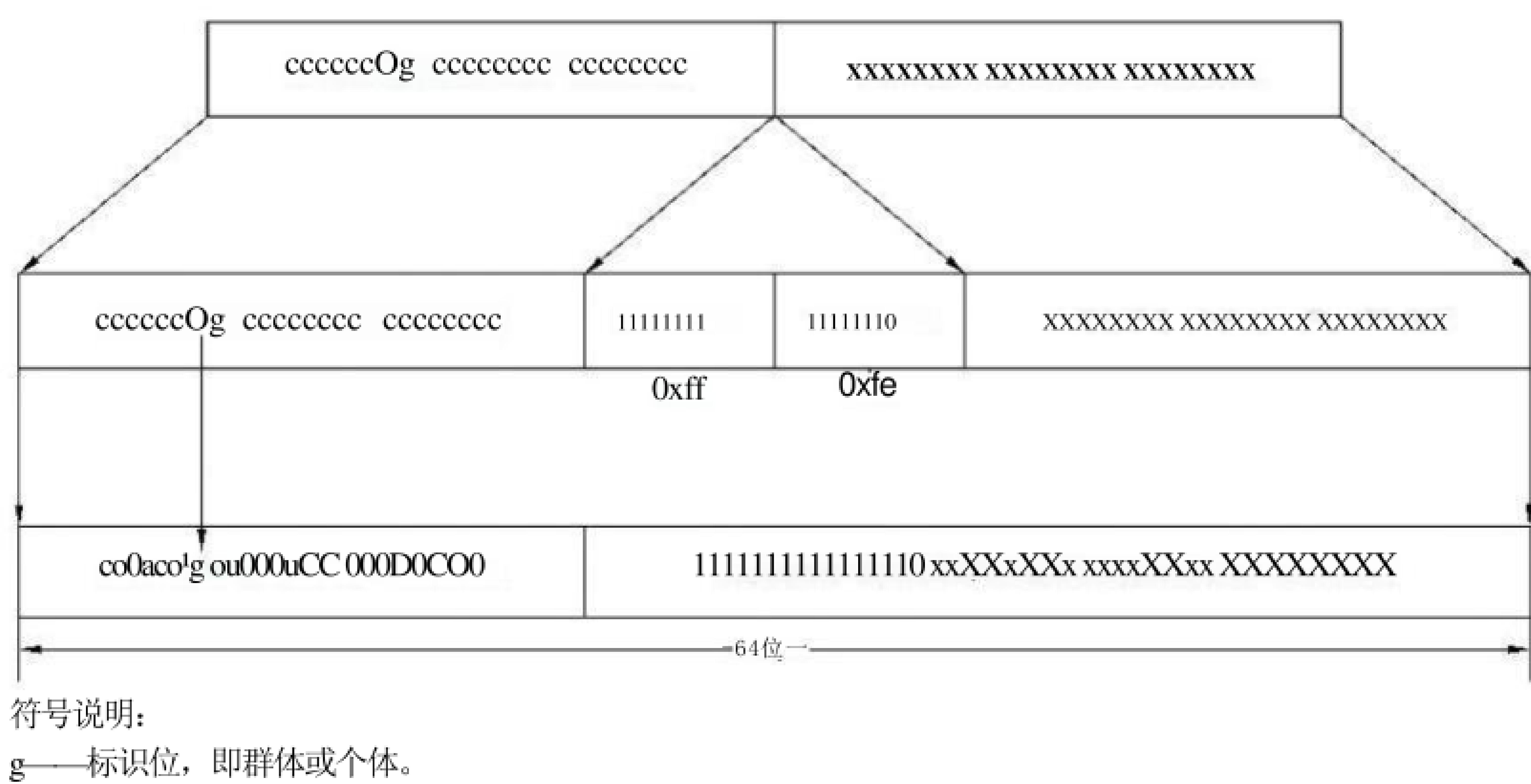


图 2 EUI-64 接口标识符编码方法

6.2 加密变换编码方法

该编码方法适用于互联网接入服务商、应用基础设施服务商、自用网络运营者等 IPv6 地址运营实体通过DHCPv6 向网络终端分配IPv6 地址时的接口标识符编码。通过对网络终端标识进行加密变换处理后形成接口标识符，计算方法为：

IID=E（网络终端标识，前缀，随机数，计数器，保留项，鉴别码，KEY）

- 式中：
- E()——加密变换函数，为加密、杂凑等基本方法或其组合，输出为64位；
  - 网络终端标识——必选参数，用于标识网络终端，如MAC地址、IMEI等；
  - 前缀——可选参数，分配给网络终端的IPv6地址前缀，长度为64位；
  - 随机数——可选参数，随机生成的序列，用于随机化IPv6地址；
  - 计数器——可选参数，用于扩展IPv6地址的随机空间；
  - 保留项——可选参数，用于标识其他信息；
  - 鉴别码——可选参数，用于鉴别前缀等输入字段的完整性；
  - KEY——可选参数，加密算法所需的密钥或杂凑算法所需的盐值；E() 为加密算法时，KEY 为必选参数。

注1:采用不同的E(), 会产生不同的性能开销。  
注2:冲突地址校验能力通过调整随机数或计数器实现。

应能根据函数E()、KEY等参数以及生成的IID 计算出网络终端标识或与网络终端标识具有稳定对应关系的映射值。  
加密变换编码方法计算实例见附录A。

附录 A  
(资料性)  
加密变换编码方法计算实例

A.1 实例一

依据6.2, 编码方法计算为:

$$IID=Ek(ID,params)$$

式中:

- E() —— 输入输出长度为64位的密码算法, 如CAST-128、HIGHT 等;
- K —— 对称密钥, 长度要求大于或等于128位, 保证加密算法的安全性, 同时为了保证密钥的安全性, 需定期更换密钥;
- ID —— 标识网络终端的序列, 长度为m 位, 选取MAC 地址、IMEI 等网络终端标识或以上信息的杂凑截取值等;
- Params——与网络终端标识一同嵌入接口标识符的额外字段, 如计数器、时间戳等, 其长度为(64—m)位。

A.2 实例二

依据6.2, 编码方法计算为:

$$IID=E(ID, \text{保留项}, \text{随机数}, \text{鉴别码}, \text{KEY})$$

实例二的接口标识符生成步骤如下。

a) 生成64位原始编码。原始编码格式如图 A.1所示。

m位	n位	r位	(64—m—n—r) 位
ID	保留项	随机数	鉴别码

说明:

- ID —— 识网络终端的序列, 长度为m 位, 选取 MAC地址、IMEI等网络终端标识或以上信息的杂凑截取值等;
- 保留项——保留字段, 长度为n 位, 用于标识其他信息, 如地址申请时间标识等;
- 随机数——随机位, 长度为r 位, 基于时间等随机生成;
- 鉴别码——地址分发设备调用与64位地址前缀关联的密钥, 计算消息鉴别码, 取最后(64—m—n—r) 位作为鉴别码。长度为(64—m—n—r)位。消息鉴别码算法选用国密SM3-HMAC等。

图 A.1 64 位原始编码格式

b) 使用对称加密方法, 加密生成接口标识符: 地址分发设备调用与64位地址前缀关联的密钥, 将a) 生成的64位加密后作为接口标识符。密钥根据安全需求定期更换, 加密算法采用PRESENT 等64位分组长度的对称加密算法。

A.3 实例三

依据6.2, 将网络终端标识与前缀等参数的杂凑值进行异或得到接口标识符, 编码方法计算为:

$$IID=(ID||Reserved||Padding) \oplus (MSB-(m+n)(hash(Prefix,Rand,Counter,Key))||Rand)$$

- 式中：
- ID ——标识网络终端的序列，长度为 $m(m \geq 48)$  位，选取MAC 地址、IMEI 等网络终端标识或以上信息的杂凑截取值等；
- Reserved——保留字段，用于标识其他信息，长度为 $n$  位；
- Padding ——用于填充的二进制序列，长度为 $(64-m-n)$  位；
- Rand ——随机生成的二进制序列，长度为 $(64-m-n)$  位，用于随机化IPv6 地址；
- Prefix ——当前网络终端被分配的IPv6 地址网络前缀；
- Counter ——公开的计数器，长度为8位，定期更换，用于调整随机序列；
- Key ——密钥，为不低于128位的二进制序列。

注1: ||为连接运算符，功能为将两个或多个二进制序列以连接方式合并成一个二进制序列。

注2: MSB— $(m+n)$  表示取二进制序列的前 $(m+n)$  位。

接口标识符生成步骤(见图A.2) 如下：

- a) 将 ID 级联 Reserved, 填充至64位，即 $ID||Reserved||Padding$ ;
- b) 生成 $(64-m-n)$  位随机数 Rand, 然后计算 $hash(Prefix,Rand,Counter,Key)$ , 取前 $(m+n)$  位与 Rand 级联，即 $MSB-(m+n)(hash(Prefix,Rand,Counter,Key))||Rand$ ;
- c) 将 a)、b)中两个64位取值异或，结果值与当前同一子网下的有效地址接口标识符做比对，若无冲突，则作为接口标识符输出；若存在值冲突的情况，则重新生成随机数，执行步骤b)、c)。

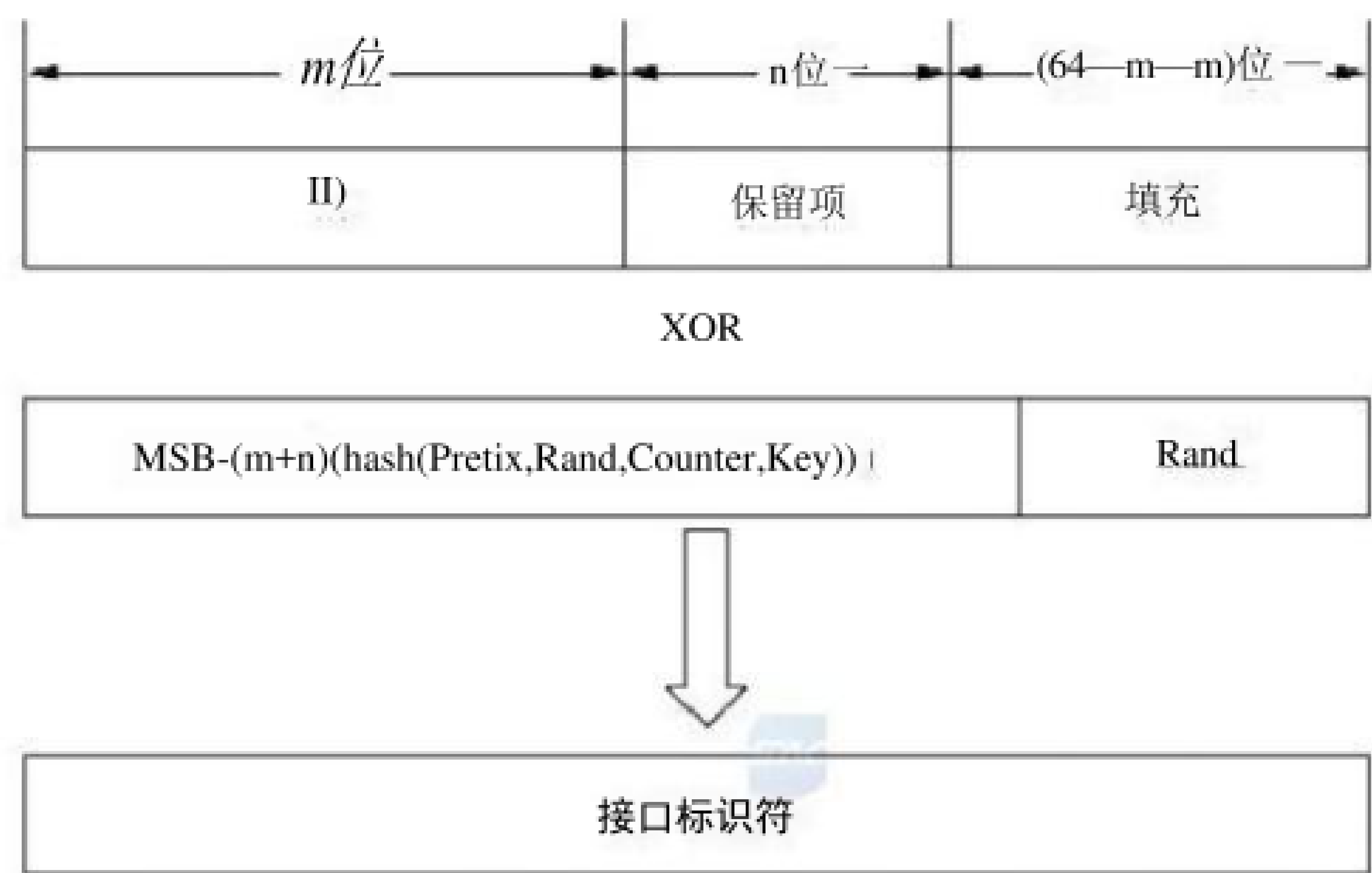


图 A.2 接口标识符生成步骤图示

实例三选择SM3 等杂凑算法。

参 考 文 献

[1]GB/T 36465—2018 网络终端操作系统总体技术要求

[2]ISO/IEC 18033-3:2010 Information technology-Security techniques—Encryption algorithms—Part 3:Block ciphers

[3] ISO/IEC 29192-2:2019 Information security—Lightweight cryptography—Part 2:Block ciphers

[4]IETF RFC 4291 IP Version 6 Addressing Architecture

[5]IETF RFC 8415 Dynamic Host Configuration Protocol for IPv6(DHCPv6)

---









[www.bzxz.net](http://www.bzxz.net)

免费标准下载网