[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04N 7/167 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200780035127.5

[43] 公开日 2009 年 8 月 26 日

[11] 公开号 CN 101518073A

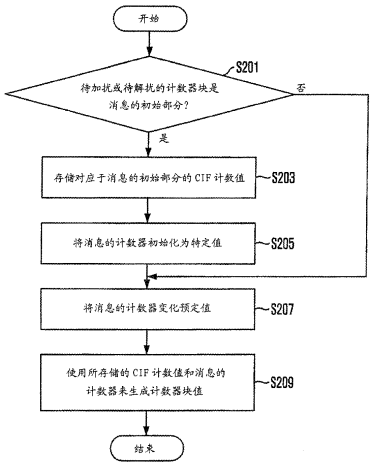
[22] 申请日 2007.7.20
[21] 申请号 200780035127.5
[30] 优先权
[32] 2006.7.20 [33] KR [31] 10-2006-0068038
[86] 国际申请 PCT/KR2007/003521 2007.7.20
[87] 国际公布 WO2008/010689 英 2008.1.24
[85] 进入国家阶段日期 2009.3.20
[71] 申请人 韩国电子通信研究院
地址 韩国大田市
[72] 发明人 李珍焕 李勇勋 咸泳权 安忠铉 李寿寅
[74] 专利代理机构 北京市柳沈律师事务所
代理人 邵亚丽
权利要求书 2 页 说明书 8 页 附图 2 页

[54] 发明名称

用于产生计数器块值的方法

[57] 摘要

提供了一种用于在不额外发送计数器块值的条件下生成计数器块值的方法。用于生成加扰器或解扰器所需要的计数器块值的方法包括以下步骤：a) 当待加扰或待解扰的计数器块在消息的初始部分中时，将该消息的计数器设置为预定的初始值；b) 当待加扰或待解扰的计数器块在消息的初始部分中时，将对应于该消息的初始部分的公共交织帧计数值存储到缓冲器中；c) 将计数器增加预定数；和 d) 通过使用在步骤 b) 中存储的 CIF 计数值和在步骤 c) 中增加后的计数器来生成计数器块值。



1. 一种用于生成加扰器或解扰器所需要的计数器块值的方法，包含下列步骤：

a）当待加扰或待解扰的计数器块在消息的初始部分中时，将该消息的计数器设置为预定的初始值；

b）当所述待加扰或待解扰的计数器块在该消息的初始部分中时，将对应于该消息的初始部分的公共交织帧 CIF 计数值存储到缓冲器中；

c）将所述计数器增加预定数；和

d）通过使用在步骤 b）中存储的 CIF 计数值和在步骤 c）中增加后的计数器来生成计数器块值。

2. 如权利要求 1 所述的方法，其中，所述 CIF 计数值是包含在传输帧的快速信息组 FIG 中的 CIF 计数值的全部或部分。

3. 如权利要求 1 所述的方法，其中，所述 CIF 计数值是包含在条件访问同步参数 CASyncParam 中的 CIF 计数值的全部或部分。

4. 一种用于生成加扰器或解扰器所需要的计数器块值的方法，该方法包括以下步骤：

a）当待加扰或待解扰的计数器块在消息的初始部分中时，将该消息的计数器设置为预定的初始值；

b）当所述待加扰或待解扰的计数器块在该消息的初始部分中时，将条件访问同步参数 CASyncParam 上携带的该消息的标识符存储到缓冲器中；

c）将所述计数器增加预定数；和

d）通过使用在步骤 b）中存储的所述消息的标识符和在步骤 c）中增加后的计数器来生成计数器块值。

5. 一种用于生成加扰器或解扰器所需要的计数器块值的方法，该方法包括以下步骤：

a）当待加扰或待解扰的计数器块在消息的初始部分中时，将该消息的计数器设置为预定的初始值；

b）当所述待加扰或待解扰的计数器块在该消息的初始部分中时，将初始化计数器块值存储到缓冲器中；

c）将所述计数器增加预定数；和

d）通过使用在步骤b）中存储的初始化计数器块值和在步骤c）中增加后的计数器来生成计数器块值。

6. 如权利要求5所述的方法，其中，所述初始化计数器块值包含在每条消息的条件访问前缀中并且被发送。

7. 一种用于生成加扰器或解扰器所需要的计数器块值的方法，该方法包括以下步骤：

a）从接收到的数据或待发送的数据中提取第一个值；

b）生成针对单位消息的每个计数器块而改变的第二个值；和

c）通过使用所述第一个值和所述第二个值来生成计数器块值。

8. 如权利要求7所述的方法，其中，在步骤c）中，在比特水平上简单地组合所述第一个值和第二个值。

9. 如权利要求8所述的方法，其中，所述第一个值形成计数器块值的最高有效位MSB，而所述第二个值形成计数器块值的最低有效位LSB。

10. 如权利要求7所述的方法，其中，在步骤c）中，对所述第一个值和第二个值执行预定运算。

11. 如权利要求7所述的方法，其中，所述第一个值是对应于消息的初始部分的公共交织帧CIF计数值。

12. 如权利要求7所述的方法，其中，所述第一个值是包含在条件访问同步参数中的值。

13. 如权利要求12所述的方法，其中，所述第一个值是所述消息的标识符。

14. 如权利要求12所述的方法，其中，所述第一个值是初始化计数器值。

15. 如权利要求7所述的方法，其中，以消息为单位初始化所述第二个值。

16. 如权利要求15所述的方法，其中，对于所述单位消息的每一个计数器块，所述第二个值改变预定值那么多。

用于产生计数器块值的方法

技术领域

本发明涉及用于产生计数器块值的方法；并且，更具体来说，涉及用于简单处理计数器块值而无需额外发送/接收计数器块值的方法。

本工作部分地由韩国信息与通信部（MIC）和韩国通信技术发展研究院（IITA）的信息技术（IT）研究与开发项目支持（2005-S-403-2，“Development of Super-intelligent Multimedia Anytime-anywhere Realistic TV (SmarTV) Technology”）。

背景技术

基于 Eureka-147 的数字音频广播(DAB)不仅提供了数字音频广播业务，而且还提供了多种多样的多媒体业务，诸如幻灯片、广播网站、交通和游客信息业务。用于提供带有运动图像视频业务的基于 Eureka-147 的 DAB 技术的标准和技术就是数字多媒体广播（DMB）标准和技术。

Eureka-147 的帧结构包括音频业务部分、视频业务部分和数据业务部分。有关各项业务的信息按 24 毫秒为单位帧被多路复用和传输。

DMB 传输帧由同步信道、快速信息通道（Fast Information Channel，FIC）和主要业务信道（Main Service Channel，MSC）组成。

FIC 包括多个快速信息块（Fast information block，FIB），MSC 包括多个公共交织帧（Common interleaved frame，CIF）。

CIF 包括视频数据和音频数据，FIB 包括有关 CIF 中所包含的数据的结构的信息。每一个 FIG 均包括快速信息组（Fast information group，FIG），其传输用来设置用于条件访问（conditional access）的参数的信号。每个传输帧的第一个 FIB 包括 CIF 计数信息。换句话说，CIF 计数信息是通过被携带在 FIG 上而被传输的。CIF 计数信息用于计算相应的 CIF 计数值并且数据以 CIF 为单位被编码/解码。CIF 计数值为 13 位长并且计数器以 5000 二进制

数来工作(operate in a 5000 binary)。

并且，条件访问同步参数（CASyncParam）被用于在接收器中对消息进行解扰的处理过程，以将该消息与解扰器（descrambler）或者接收器的其它功能同步。条件访问同步参数（CASyncParam）是通过携带在待加扰或待解扰的消息的前缀上而被传输的。条件访问参数（CASyncParam）传递消息标识符以及表示控制字和 CIF 计数值的变化的切换（toggle）信息。

由条件访问系统（CAS）中的接收器确定特定内容是否是可访问的。那些为内容付费的用户可以使用条件访问系统中的内容。

一般说来，条件访问系统需要以下功能：加扰和解扰功能，用于保护内容不受未授权用户的侵害；授权(entitle)控制功能和授权管理功能，用于仅向那些已经进行了预定付费的用户提供内容。

首先，加扰是一项用于使用控制字（CW）使内容变形以便保护内容不受未授权用户侵害的技术。发送器需要加密，以便保护要发送到接收器的解密器的加扰内容和控制字。接收器需要发送器所拥有的相同密钥(secret key)，以执行解扰。

授权控制是一项用于对控制字进行加密的技术。经加密的控制字是通过携带在授权控制消息（ECM）上而被发送到接收器的。为了安全起见，周期性地发送授权控制消息，并且所发送的授权控制消息包括经加密的控制字。授权控制消息还包括控制参数。接收器将包含在所发送的授权控制消息中的控制参数与存储在接收器中的授权参数进行比较，确定用户是否具有访问内容的权限。当确定该用户具有访问权限时，接收器使用密钥将控制字解密并且使用经解密的控制字对接收到的内容解扰。

为了使用块加密的计数器模式来对加扰器和解扰器中的内容进行加密和解密，需要控制字和对于每个计数器块都不同的计数器块值。

与此同时，作为用于地面 DMB 内容的条件访问的国际标准的欧洲电信标准研究院（European Telecommunication Standards Institute，ETSI）技术规范（TS）102 367 根据加扰（scrambling）方法定义了三种条件访问模式：子信道条件访问、数据组条件访问和多媒体对象传输（Multimedia Object Transfer，MOT）条件访问。

针对内容中的每条消息执行加扰和解扰。从而，一条待加扰的消息应当

被连续处理，并且用于加扰或解扰一条消息的控制字应当不被改变。在地面DMB 内容中，待加扰或待解扰的消息的长度是不同的并且消息传输周期也不是相同的。在子信道条件访问模式的情况下，消息发送/接收周期与 CIF 一样，都是 24 毫秒。在数据组条件访问模式和 MOT 条件访问模式的情况下，消息发送/接收周期不是规则的并且可以通过一个或多个 CIF 发送/接收消息。

加扰方法被分为两种类型：块加密和流加密。就安全性而言，诸如高级加密标准（Advanced Encyption Standard，AES）这样的块加密方法要优于流加密。

作为使用块加密方法的推荐标准的美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）特别公开(Special Publication)800-38A 建议了五种 AES 标准运算模式。具体说来，NIST 特别公开 800-38A 定义了下列五种模式：电子密码本（Electric Code Book，ECB）模式、密文块链接（Cipher Block Chaining，CBC）模式、密文反馈(Cipher Feedback, CFB)模式、输出反馈(Output Feedback, OFB)模式和计数器（CTR）模式。本发明涉及这五种块加密方法中的计数器模式。

NIST 特别公开 800-38A 建议了两种用于设置待加扰的消息的计数器块值的方法。这里，计数器块值表示为每个块不同地给出的值，用于在计数器模式下执行加扰或解扰。根据加扰器中使用的块加密的计数器模式，消息被划分为多个块并且这些块被加扰。

根据第一种方法，消息的第一个计数器块值是通过将预定数加到前一条消息的最后一个计数器块值上而得到的值。换句话说，第一条消息的第一个计数器块值被初始化为“0”并且对每个块增加“1”的值被用作计数器块值。第二条消息的第一个计数器块值是通过向第一条消息的最后一个计数器块值加“1”而得到的值。

但是，当用户改变信道时，上述方法不能正常地将内容呈现给用户，这是因为改变后的信道需要新的控制字，并且直到新的控制字被接收到，才能得知计数器块值。简而言之，该方法具有这样的缺点：每当信道改变时，用户必须等待，直到接收到新的控制字。

第二种方法对于计数器块的一半比特部分（a half-bit part）与第一种方

法类似。每条消息的第一个计数器块值被初始化为“0”，并且在一条消息中每个后续的计数器块值增加“1”。计数器块的另一半比特部分包括标识符，它的值与其它消息不重叠。但是，第二种方法也有个问题：频率被消耗用于将标识符发送到接收器，以使得每条消息具有不同的标识符。

图 1 示出用于传统加扰器/解扰器中的块加密的计数器模式。参见图 1，加扰器使用控制字对内容进行加扰，该内容为计数器块序列，并且控制字以数秒到数十秒为周期变为不同的随机数，以防止受到黑客侵害。

根据被用作加扰器的块加密的计数器模式，内容被划分为多个块并被加扰。只要使用相同的控制字，块的计数器值（这里将被称作计数器块值）就应当是互不相同的。因此，当将内容划分为 n 个块并且使用相同的控制字进行加扰时，就需要 n 个不同的计数器块值。

加扰器的密文 111、112、...11n 使用控制字和计数器块值输出用于各个计数器块的加密数据，所述计数器块值对于各个块互不相同。加扰器的 XOR 运算器 121、122、...12n 对经加密的输出数据和被分为 n 块的未加扰的计数器块执行 XOR 运算。加扰器中 XOR 运算器的运算结果为加扰后的内容。

解扰器的译文 131、132、...13n 使用加扰器所使用的相同的计数器块值和控制字对加扰后的内容进行解密。这里，密文有两种类型。一种是前向密文（forward cipher），另一种是后向密文（backward cipher）。计数器模式中所使用的解扰器的译文与加扰器的前向密文相同。

块加密的计数器模式需要从发送器发送控制字和计数器块值到接收器，并且频率被用于发送计数器块值，该计数器块值对于各个计数器块互不相同。因此，就使用频率而言，这样的效率很低。

因此，为了不额外地发送计数器块值，需要开发一种在使用相同控制字的同时生成遍及所有块都不重复的计数器块值的方法。

发明内容

技术问题

本发明的实施例旨在提供一种为了在加扰或解扰处理过程中不额外地发送计数器块值而在使用相同控制字的同时生成遍及所有块都不重复的计数器块值的方法。

技术方案

依照本发明的一个方面，其被设计为用于满足此需求，提供一种用于在不额外发送或接收计数器块值的同时简单地处理计数块值的方法。

有益效果

本发明的方法通过组合 CIF 计数值和计数器来生成计数器块值。由于不额外地发送计数器块值，因而能够提高频率使用效率。

附图说明

图 1 示出了在传统加扰器和解扰器中使用的块加密的计数器模式。

图 2 是描述了依照本发明的实施例的、用于生成加扰器或解扰器中所需要的计数器块值的方法的流程图。

具体实施方式

依照本发明的一个方面（被设计为用于实现目的），提供一种用于生成加扰器或解扰器所需要的计数器块值的方法，该方法包括以下步骤：a）当待加扰或待解扰的计数器块在消息的初始部分中时，将该消息的计数器设置为预定的初始值；b）当待加扰或待解扰的计数器块在消息的初始部分中时，将对应于该消息的初始部分的公共交织帧（Common Interleaved Frame，CIF）计数值存储到缓冲器中；c）将计数器增加预定数；和 d）通过使用在步骤 b）中存储的 CIF 计数值和在步骤 c）中增加后的计数器来生成计数器块值。

依照本发明的另一个方面（被设计为用于实现目的），提供一种用于生成加扰器或解扰器所需要的计数器块值的方法，该方法包括以下步骤：a）当待加扰或待解扰的计数器块在消息的初始部分中时，将该消息的计数器设置为预定的初始值；b）当待加扰或待解扰的计数器块在消息的初始部分中时，将条件访问同步参数（CASyncParam）上携带的消息的标识符存储到缓冲器中；c）将计数器增加预定数；和 d）通过使用在步骤 b）中存储的消息的标识符和在步骤 c）中增加后的计数器来生成计数器块值。

依照本发明的又一个方面（被设计为用于实现目的），提供一种用于生成加扰器或解扰器所需要的计数器块值的方法，该方法包括以下步骤：a）当待加扰或待解扰的计数器块在消息的初始部分中时，将该消息的计数器设

置为预定的初始值；b）当待加扰或待解扰的计数器块在消息的初始部分中时，将初始化计数器块值存储到缓冲器中；c）将计数器增加预定数；和 d）通过使用在步骤 b）中存储的初始化计数器块值和在步骤 c）中增加后的计数器来生成计数器块值。

依照本发明的又一个方面（被设计为用于实现目的），提供一种用于生成加扰器或解扰器所需要的计数器块值的方法，该方法包括以下步骤：a）从接收到的数据或待发送的数据中提取第一个值；b）生成针对单位消息的每个计数器块而改变的第二个值；和 c）通过使用第一个值和第二个值来生成计数器块值。

而且，第一个值可以是对应于消息的初始部分的公共交织帧（CIF）计数值或者包含在条件访问同步参数中的值。包含在条件访问同步参数中的值的例子为消息的标识符和初始化计数器值。

与此同时，以消息为单位初始化第二个值，并且对于单位消息的计数器块中的每个块，第二个值变化预定值那么多。

本发明的优点、特征和方面将从下文中将阐述的结合附图对实施例的以下描述中变得明显。

一般说来，控制字以数秒到数十秒为间隔地变化，公共交织帧（CIF）计数值每 24 毫秒增加“1”。由于 CIF 计数值的增长期比控制字的变化期短，因而 CIF 计数值可以用于计数器块值的一部分。此外，能够通过携带在条件访问同步参数（CASyncParam）上进行传输的消息的标识符也可以取代 CIF 计数值而用于计数器块值的一部分。

根据本发明的实施例，在地面 DMB 内容的条件访问模式中所定义的初始化计数器块值可以如消息的标识符那样取代 CIF 计数值而用于计数器块值的一部分，所述条件访问模式为子信道加扰模式、数据组加扰模式和 MOT 加扰模式。具体来说，初始化计数器块值包含在用于每个消息的条件访问前缀（CAPrefix）并且以地面 DMB 条件访问方法传送。在情况 1）子信道加扰模式下，当填充分组指示符（padding packet indicator）为“0”时，初始化计数器块值可以被放置在第二字节和第三字节中，或者当填充分组指示符为“1”时，初始化计数器块值可以被放置在第三字节和第四字节中。在情况 2）数据组加扰模式下，初始化计数器块值可以被放置在第一字节中。在

情况 3）MOT 加扰模式下，初始化计数器块值可以被放置在第一字节和第二字节中。

图 2 是描述依照本发明的实施例，用于生成加扰器或解扰器中所需要的计数器块值的方法的流程图。该图示出了使用 CIF 计数值的实施例。这里，初始化计数器块值而非 CIF 计数值，可以被用作消息的标识符。

参见图 2，当输入消息时，在步骤 S201 中确定待加扰或待解扰的计数器块是否是消息的初始部分。

在步骤 S203 中，存储对应于消息的初始部分的 CIF 计数值。

在步骤 S205 中，当计数器块是消息的初始部分时，消息的计数器被初始化为预定的初始值。

随后，在步骤 207 中，被初始化的消息的计数器改变预定值。例如，计数器可以增加用于单位消息的每个计数器块的预定值那么多。

与此同时，当计数器块不是消息的初始部分时，计数器改变，例如，在步骤 207 中增加用于单位消息的每个计数器块的预定值那么多。

随后，在步骤 S209 使用所存储的 CIF 计数值和被增加了预定值的消息的计数器来生成计数器块值。可以通过简单地组合所存储的 CIF 计数值和被增加了预定值的消息的计数器，或者通过执行预定运算，来生成计数器块值。这里，当确定计数器块不是消息的初始部分时，所存储的 CIF 计数值就是对应于消息的初始部分的 CIF 计数值。例如，当生成 128 位的计数器块值时，13 个最高有效位（MSB）使用 CIF 计数值，而其余的 115 个最低有效位（LSB）使用消息的计数器。

通过上述方法生成每个块的计数器块。因此，可以在不发送计数器块值的条件下生成加扰器和解扰器中所使用的计数器块值。

上面所描述的本发明的方法可以被实现为程序并且被存储在计算机可读记录介质中，诸如 CD-ROM、RAM、ROM、软盘、硬盘和磁光盘中。由于本领域技术人员可以很容易地实现该过程，因此这里不再提供进一步的描述。

尽管已经就特定的优选实施例描述了本发明，但是本领域的技术人员将很清楚，在不脱离如后附权利要求书中所限定的本发明的精神和范围的前提下，可以进行各种变化和修改。

工业上的可应用性

本发明提供了一种在加扰或解扰处理过程中在不额外发送计数器块值的条件下，只要使用相同的控制字就生成贯穿消息的所有块都不重复的计数器块值的方法。

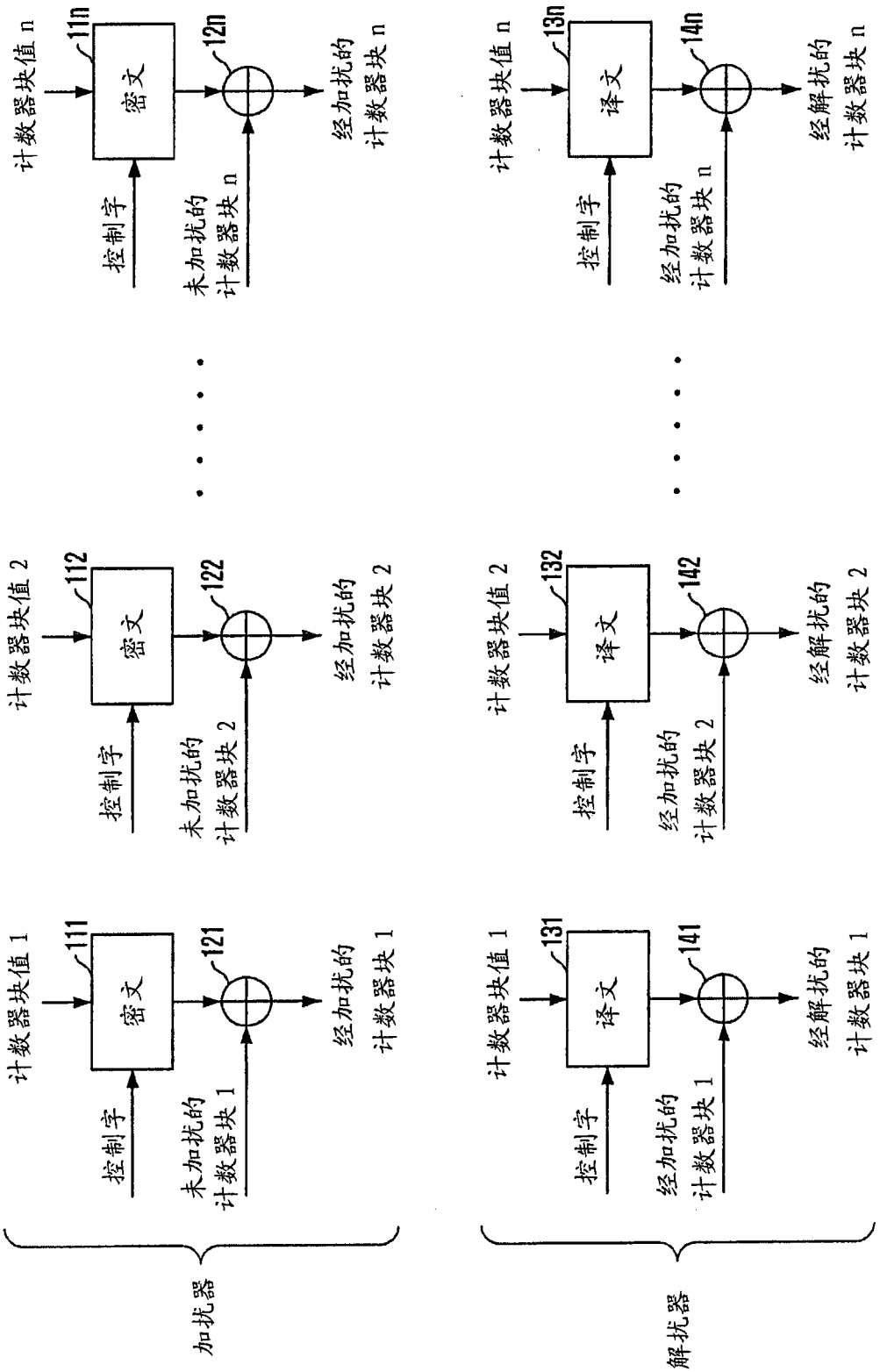

计数器块值 1
111
密文
控制字
未加扰的
计数器块 1
121
经加扰的
计数器块 1
计数器块值 2
112
密文
控制字
未加扰的
计数器块 2
122
经加扰的
计数器块 2
计数器块值 n
11n
密文
控制字
未加扰的
计数器块 n
12n
经加扰的
计数器块 n
加扰器
计数器块值 1
131
译文
控制字
经加扰的
计数器块 1
141
经解扰的
计数器块 1
计数器块值 2
132
译文
控制字
经加扰的
计数器块 2
142
经解扰的
计数器块 2
计数器块值 n
13n
译文
控制字
经加扰的
计数器块 n
14n
经解扰的
计数器块 n
解扰器

图 1

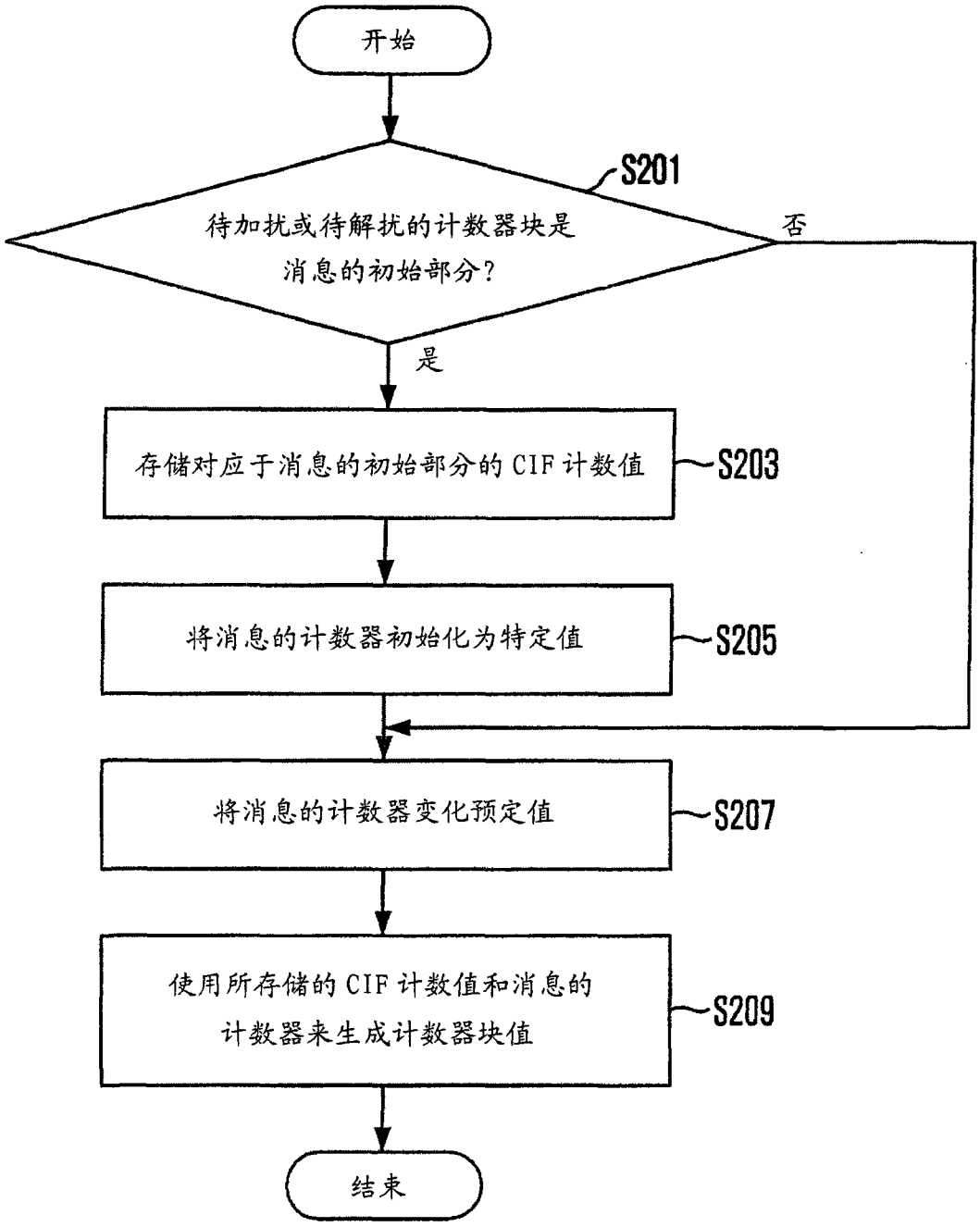

开始
S201
待加扰或待解扰的计数器块是消息的初始部分？
否
是
存储对应于消息的初始部分的 CIF 计数值
S203
将消息的计数器初始化为特定值
S205
将消息的计数器变化预定值
S207
使用所存储的 CIF 计数值和消息的计数器来生成计数器块值
S209
结束

图 2