[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
H04L 9/06 (2006.01)

[12] 发明专利说明书

专利号 ZL 01821337.5

[45] 授权公告日 2008 年 10 月 22 日

[11] 授权公告号 CN 100428751C

[22] 申请日 2001.12.10 [21] 申请号 01821337.5
[30] 优先权
[32] 2000.12.25 [33] JP [31] 391938/00
[86] 国际申请 PCT/JP2001/010804 2001.12.10
[87] 国际公布 WO2002/052765 英 2002.7.4
[85] 进入国家阶段日期 2003.6.25
[73] 专利权人 松下电器产业株式会社
地址 日本大阪府
[72] 发明人 太田雄策 山口雅史 山内弘贵
[56] 参考文献
WO0002406A2 2000.1.13
WO9956434A1 1999.11.4
审查员 刘冀鹏

[74] 专利代理机构 永新专利商标代理有限公司
代理人 蹇 炜

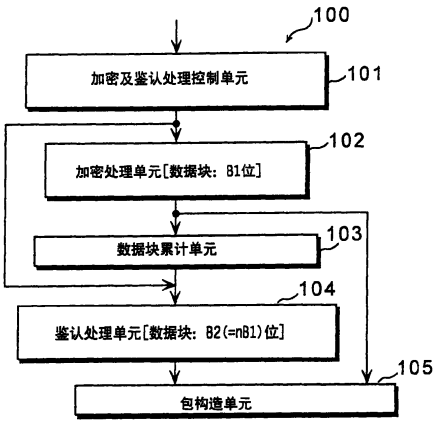
权利要求书 6 页 说明书 37 页 附图 18 页

[54] 发明名称

安全通信包处理装置及其方法

[57] 摘要

一种安全通信包处理装置(100)包括：加密处理单元(102)，它按照 B1 位的数据块单元来执行加密处理与解密处理；鉴认处理单元(104)，它按照 B2(=n ×B1)位的数据块单元来与该加密处理单元(102)中的加密处理或解密处理并行执行鉴认处理并输出该鉴认值；数据块累计单元(103)，它累计来自加密处理单元(102)的数据块，并在这些数据块的累计值达到 B2 位时将这些数据块输出到鉴认处理单元(104)；包构造单元(105)，它采用来自加密处理单元(102)的数据块与来自鉴认处理单元(104)的鉴认值重新构造一个包；以及加密及鉴认处理控制单元(101)，它将该输入包划分为 B1 位数据块，并将这些数据块按顺序输出到该加密处理单元。



1、一种安全通信包处理装置，用于对一个包执行加密处理、解密处理与鉴认处理中至少一项处理，包括：

一个或多个加密处理单元，其运行以便按照一个 B1 位数据块单元来执行该加密处理与该解密处理；

一个或多个鉴认处理单元，其运行以便按照一个 B2 位数据块单元来与该加密处理单元的加密处理或解密处理并行地执行该鉴认处理，而且输出一个标志该鉴认处理结果的鉴认值，其中 $B2= n \times B1$，n 为正整数；

一个或多个数据块累计单元，其运行以便累计由该加密处理单元对其执行加密处理的数据块，而且在这些数据块的累计值达到 B2 位时，将这些数据块输出到该鉴认处理单元；

一个包构造单元，其运行以便从该加密处理单元接收这些加密的或解密的数据块，从该鉴认处理单元接收该鉴认值，而且构造一个包含该接收到的数据块以及鉴认值的包；以及

一个控制单元，其运行以便将该输入包划分为 B1 位的数据块，而且将这些数据块按顺序输出到该加密处理单元；

其中该控制单元判断该输入包属于哪种类型，即是需要该加密处理与该鉴认处理的第一类型的包、需要该解密处理与该鉴认处理的第二类型的包、需要该加密处理与该解密处理中的一项处理的第三类型的包、或者是只需要该鉴认处理的第四类型的包，

如果该包被判定为第一类型的包，那么就将该包划分为 B1 位的数据块，而且将这些数据块按顺序输出到该加密处理单元，

如果该包被判定为第二类型的包，那么就将该包划分为 B1 位的数据

块，将它们按顺序输出到该加密处理单元，将该包或该包的复制品划分为B2位的数据块，而且将这些数据块按顺序输出到该鉴认处理单元，

如果该包被判定为第三类型的包，那么就将该包划分为 B1 位的数据块，而且将这些数据块按顺序输出到该加密处理单元，而且

如果该包被判定为第四类型的包，那么就将该包划分为 B2 位的数据块，而且将这些数据块按顺序输出到该鉴认处理单元。

2、按照权利要求 1 的安全通信包处理装置，

其中该加密处理单元与该鉴认处理单元中至少一种单元的数量为 2 或更多，而且

该数据块累计单元的数量等于该加密处理单元的数量。

3、按照权利要求 2 的安全通信包处理装置，

其中该控制单元在两个或两个以上的加密处理单元或者两个或两个以上的鉴认处理单元中指定准备进行处理的加密处理单元或者鉴认处理单元，而且将这些数据块输出到该指定的加密处理单元或者鉴认处理单元。

4、按照权利要求 1 的安全通信包处理装置，还包括：

一个数据通道连接切换单元，它能够分别并且独立地连接该控制单元的输出与该加密处理单元的输入、该控制单元的输出与该鉴认处理单元的输入、该加密处理单元的输出与该数据块累计单元的输入以及该数据块累计单元的输出与该鉴认处理单元的输入。

5、按照权利要求 4 的安全通信包处理装置，

其中该控制单元判断该输入的包属于哪一种类型，即是需要该加密处理与该鉴认处理的第一类型的包，需要该解密处理与该鉴认处理的第二类型的包，需要该加密处理与该解密处理中的一项处理的第三类型的包，或

者是只需要该鉴认处理的第四类型的包，

如果该包被判定为该第一类型的包，那么就控制该数据通道连接切换单元以便连接该控制单元的输出与该加密处理单元的输入、该加密处理单元的输出与该数据块累计单元的输入以及该数据块累计单元的输出与该鉴认处理单元的输入，

如果该包被判定为该第二类型的包，那么就控制该数据通道连接切换单元以便连接该控制单元的输出与该加密处理单元的输入以及该控制单元的输出与该鉴认单元的输入，

如果该包被判定为该第三类型的包，那么就控制该数据通道连接切换单元以便连接该控制单元的输出与该加密处理单元的输入，而且

如果该包被判定为该第四类型的包，那么就控制该数据通道连接切换单元以便连接该控制单元的输出与该鉴认处理单元的输入。

6、按照权利要求 5 的安全通信包处理装置，

其中该加密处理单元与该鉴认处理单元中至少有一种单元的数量为 2 或更多，而且

该数据块累计单元的数量等于该加密处理单元的数量。

7、按照权利要求 6 的安全通信包处理装置，

其中该控制单元在两个或两个以上的加密处理单元或者两个或两个以上的鉴认处理单元中指定准备进行处理的加密处理单元或者鉴认处理单元，而且使该数据通道连接切换单元执行对该指定的加密处理单元或者鉴认处理单元的连接。

8、按照权利要求 1 的安全通信包处理装置，还包括：

一个处理数据保存单元，对该加密处理单元、鉴认处理单元以及数据

块累计单元中至少一种单元的每一个，它都具有一个分别与该处理单元对应的存储器区域以供暂时保存正在该处理单元中处理的数据块。

9、按照权利要求 8 的安全通信包处理装置，

其中该控制单元在这些处理单元中指定正在对具有最低优先级的包的数据块执行处理的处理单元，而且当正在该处理单元中处理的数据块被保存到该处理数据保存单元之后，使该处理单元执行该输入包的数据块的处理。

10、按照权利要求 9 的安全通信包处理装置，还包括：

数据通道连接切换单元，可分别并且独立地连接该控制单元的输出与该加密处理单元的输入、该控制单元的输出与该鉴认处理单元的输入、该加密处理单元的输出与该数据块累计单元的输入以及该数据块累计单元的输出与该鉴认处理单元的输入。

11、按照权利要求 10 的安全通信包处理装置，

其中该加密处理单元与该鉴认处理单元中至少有一种单元的数量为 2 或更多，而且

该数据块累计单元的数量等于该加密处理单元的数量。

12、按照权利要求 1 的安全通信包处理装置，还包括：

处理数据保存单元，对该加密处理单元、鉴认处理单元以及数据块累计单元中至少两种单元的每一个，它都具有一个由这些处理单元共享的存储器区域以供暂时保存正在这些处理单元中处理的数据块。

13、按照权利要求 12 的安全通信包处理装置，

其中该控制单元在这些处理单元中指定正在对包的数据块执行处理的处理单元具有最低优先级，而且当正在该处理单元中处理的数据块被保存

到该处理数据保存单元之后，使该处理单元执行该输入包的数据块的处理。

14、按照权利要求 13 的安全通信包处理装置，还包括：

数据通道连接切换单元，可分别并且独立地连接该控制单元的输出与该加密处理单元的输入、该控制单元的输出与该鉴认处理单元的输入、该加密处理单元的输出与该数据块累计单元的输入以及该数据块累计单元的输出与该鉴认处理单元的输入。

15、按照权利要求 14 的安全通信包处理装置，

其中该加密处理单元与该鉴认处理单元中至少有一种单元的数量为 2 或更多，而且

该数据块累计单元的数量等于该加密处理单元的数量。

16、按照权利要求 1 的安全通信包处理装置，

其中该 B1 是 64，而且

该 B2 是 512。

17、一种安全通信包处理方法，用于对该包执行加密处理、解密处理与鉴认处理中至少一项处理，包括：

划分步骤，用来将该输入包划分为 B1 位的数据块；

加密处理步骤，用来对这些划分后的 B1 位的数据块执行加密处理或解密处理；

数据块累计步骤，用来累计这些加密数据块，并且在这些数据块的累计值达到 B2 位时输出这些数据块，其中 $B2 = n \times B1$，n 为正整数；

鉴认处理步骤，用来与该加密处理或解密处理并行地对这些输出的 B2 位数据块执行鉴认处理，而且输出标志该鉴认处理结果的鉴认值；

包构造步骤，用来接收这些加密的或解密的数据块，接收该鉴认值，

而且构造包括这些接收到的数据块以及该鉴认值的包；

控制步骤，用来判断该输入包是哪一种类型，即，是需要该加密处理与该鉴认处理的第一类型的包、需要该解密处理与该鉴认处理的第二类型的包、只需要该加密处理与该解密处理中的一项处理的第三类型的包或者是只需要该鉴认处理的第四类型的包，以及，如果被判定为该第一类型的包，那么就进行控制以便执行该划分步骤中的划分、该加密处理步骤中的加密处理、该数据块累计步骤中的累计、该鉴认处理步骤中的鉴认处理以及该包构造步骤中的构造。

安全通信包处理装置及其方法

技术领域

本发明涉及利用一个数据包进行保密通信的一种安全通信包处理装置及其方法，更具体地讲，涉及在保证安全的处理中加快速度及降低迟延的技术。

背景技术

随着这些年来 TCP/IP 网络（譬如互联网）的迅速普及，各种网络交易方法也已经一个接一个地使人瞩目并发展起来，譬如网上电子音乐发行及销售。尽管这类网络交易的主要前提是保证在一个服务供应商与一位用户之间存在安全可靠的交易，但互联网通常被认为是一种不安全的网络，因为它始终有被解密高手侦听与伪装的危险。所以，网络安全技术，譬如电子鉴认、通信数据加密与防火墙就引起了人们的注意。尽管这些技术一直主要通过软件来实现，但是在 TCP/IP 基础设施中，通过硬件（譬如加密处理芯片与加密电路板）来实现高速处理的需求也在为未来更宽的通信信道范围进行准备的过程中逐步增加。

在一个具有安全通信功能——譬如 IPSec（IP 安全协议套件）——的计算机或网络连接设备中，对一个既需要加密处理又需要鉴认处理的包的传统处理过程按照图 1 所示的流程图执行。对一个需要加密处理（步骤 701）的包（譬如一个 IP 包），在一个明文本包首先被划分为供加密处理的数据块（步骤 702）并且执行了这些数据块的加密处理（步骤 703）之后，它们会被重新构造成一个加密包（步骤 704）。然后，如果该包需要鉴认处理（步

骤 705），那么在该加密包被划分为供鉴认处理的数据块（步骤 706）并且执行了这些数据块的鉴认处理（步骤 707）之后，它们再被重新构造成一个鉴认处理后的包（步骤 708）。

然而，根据上述方法，对既需要加密处理又需要鉴认处理的包，必须两次执行包构造处理（图 1 的步骤 704 与步骤 708）。所以，在既需要执行该加密处理又需要执行该鉴认处理时就会出现一个问题，即一个加密处理单元或一个鉴认处理单元的处理速度下降、处理能力降低以及使用效率变差。根据这个方法还存在一个问题，那就是在处理另一个包的过程中，应当被优先处理的一个明文本包不能被优先处理。此外，在只分别安装了一个加密处理单元与鉴认处理单元的时候还存在一个问题，即不可能通过同时处理多个包来获得高速处理能力。

发明内容

所以，本发明的一个第一目的是根据上述问题提供一种安全通信包处理装置，该装置能够在既执行加密处理又执行鉴认处理时，加快处理速度、降低处理迟延、增加处理能力，并能够有效地利用该加密处理单元与该鉴认处理单元。

而且，本发明的第二目的是提供一种安全通信包处理装置，该装置能够对多个包同时而且并行执行至少加密（或解密）处理与鉴认处理中的一项处理。

此外，本发明的第三目的是提供一个具有高处理效率的安全通信包处理装置，该装置能够通过只利用一个或多个加密处理单元以及鉴认处理单元中与包类型对应的一个必要的处理单元来执行处理。

此外，本发明的第四目的是提供一个安全通信处理装置，该装置能够

控制一个包的优先级处理来进行加密（包括解密）处理与鉴认处理。

上述第一目的可以通过符合本发明的安全通信包处理装置来实现，这是具有安全通信功能的一个网络连接设备或者一台计算机，它包括一个用于对数据块进行加密处理的加密处理单元、一个用于对数据块进行鉴认处理的鉴认处理单元以及一个加密及鉴认处理控制单元，该控制单元被用来向该加密处理单元输出供加密处理的数据块以及进行该加密处理所必须的信息、向该鉴认处理单元输出供鉴认处理的数据块以及进行该鉴认处理所必须的信息、而且控制该加密处理单元与鉴认处理单元，其中，已经在该加密处理单元中经过处理的这些数据块被累计直到它们的累计值达到供该鉴认处理的最小数据块大小为止，该装置还包括一个数据块累计单元，在该累计值达到供该鉴认处理的最小数据块大小时，该数据块累计单元向该鉴认处理单元输出该累计值，在该鉴认处理单元处理从该数据块累计单元输出的数据块的同时，该加密处理单元对供下一次加密处理的数据块执行处理，而且数据块累计单元为该下一次鉴认处理累计数据块。结果，通过使该加密处理或鉴认处理所必须而且足供处理的数据块成为需要加密处理与鉴认处理的包的一个处理单元，就能够降低该处理迟延、改进该处理能力、而且有效地利用该加密处理单元与该鉴认处理单元。

具体地，按照本发发明的安全通信包处理装置可用于对一个包执行加密处理、解密处理与鉴认处理中至少一项处理，包括：

一个或多个加密处理单元，其运行以便按照一个 B1 位数据块单元来执行该加密处理与该解密处理；

一个或多个鉴认处理单元，其运行以便按照一个 B2 位数据块单元来与该加密处理单元的加密处理或解密处理并行地执行该鉴认处理，而且输出

一个标志该鉴认处理结果的鉴认值，B2= n × B1，n 是正整数；

一个或多个数据块累计单元，其运行以便累计由该加密处理单元对其执行加密处理的数据块，而且在这些数据块的累计值达到 B2 位时，将这些数据块输出到该鉴认处理单元；

一个包构造单元，其运行以便从该加密处理单元接收这些加密的或解密的数据块，从该鉴认处理单元接收该鉴认值，而且构造一个包含该接收到的数据块以及鉴认值的包；以及

一个控制单元，其运行以便将该输入包划分为 B1 位的数据块，而且将这些数据块按顺序输出到该加密处理单元；

其中该控制单元判断该输入包属于哪种类型，即是需要该加密处理与该鉴认处理的第一类型的包、需要该解密处理与该鉴认处理的第二类型的包、需要该加密处理与该解密处理中的一项处理的第三类型的包、或者是只需要该鉴认处理的第四类型的包，

如果该包被判定为第一类型的包，那么就将该包划分为 B1 位的数据块，而且将这些数据块按顺序输出到该加密处理单元，

如果该包被判定为第二类型的包，那么就将该包划分为 B1 位的数据块，将它们按顺序输出到该加密处理单元，将该包或该包的复制品划分为 B2 位的数据块，而且将这些数据块按顺序输出到该鉴认处理单元，

如果该包被判定为第三类型的包，那么就将该包划分为 B1 位的数据块，而且将这些数据块按顺序输出到该加密处理单元，而且

如果该包被判定为第四类型的包，那么就将该包划分为 B2 位的数据块，而且将这些数据块按顺序输出到该鉴认处理单元。

上述第二目的可以通过符合本发明的安全通信包处理装置来实现，其

中该加密处理单元与该鉴认处理单元中至少一种处理单元的数量为二或大于二，而且该数据块累计单元的数量等于该加密处理单元的数量。结果，多个包可以被并行处理，而且能够实现具有高处理能力的安全处理。

上述第三目的可以通过符合本发明的安全通信包处理装置来实现，该装置包括一个数据通道连接切换单元，它根据该加密及鉴认处理控制单元的处理命令，当从该加密及鉴认处理控制单元输出的数据块是供加密处理的数据块时连接该加密及鉴认处理控制单元的输出与该加密处理单元的输入，当从该加密及鉴认处理控制单元输出的数据块是供鉴认处理的数据块时连接该加密及鉴认处理控制单元的输出与该鉴认处理单元的输入，当从该加密处理单元输出的该数据块还需要鉴认处理时连接该加密处理单元的输出与该数据块累计单元的输入，而且当该数据块累计单元中累计的数据块已经可供输出时连接该数据块累计单元的输出与该鉴认处理单元的输入。结果，由于该加密处理单元、该数据块累计单元以及该鉴认处理单元并不总是需要彼此一一对应，即使存在多个加密处理单元与/或鉴认处理单元也是如此，所以在加密处理之后需要鉴认处理的数据块可以被输出到任意数据块累计单元，而且该数据块累计单元的输出可以被输出到任意鉴认处理单元。因此，该加密处理单元、该数据块累计单元以及该鉴认处理单元可以得到更有效的利用，而且该加密处理单元与该鉴认处理单元可以很容易地被替换，它们的数量也很容易增加。

上述第四目的可以通过符合本发明的安全通信包处理装置来实现，其中，根据该加密及鉴认处理控制单元的命令，在该加密处理单元、该鉴认处理单元以及该数据块累计单元的一部分单元或者所有单元中分别提供一个处理数据保存单元，用来暂时保存该加密处理单元或该鉴认处理单元中

处理的数据块、该数据块累计单元中累计的数据块以及与该数据块有关的信息。结果，该包就可以根据优先级来进行处理。

而且，在符合本发明的安全通信包处理装置中，可以对该加密处理单元、该鉴认处理单元以及该数据块累计单元的任意组合共同提供该处理数据保存单元，以便根据该加密及鉴认处理控制单元的命令来暂时保存该加密处理单元或该鉴认处理单元中处理的数据块、该数据块累计单元中累计的数据块以及与该数据块有关的信息。结果，由于连接到该处理数据保存单元的任意加密处理单元、鉴认处理单元或数据块累计单元可以采用一个共享的处理数据保存单元，而且连接到该处理数据保存单元的任意加密处理单元、鉴认处理单元或数据块累计单元可以重新开始处理该处理数据保存单元内的、处理过程中途的数据块，所以上述第四目的可以按照一种与上述安全通信包处理装置不同的结构来实现。

这里，在上述安全通信包处理装置中供加密处理的数据块可以是64位，而供鉴认处理的数据块可以是 512 位。在这种情况下，该数据块累计单元可以在它累计八个加密数据块时输出这些数据块。

另外，按照本发明的另一个方面，还提供一种安全通信包处理方法，用于对该包执行加密处理、解密处理与鉴认处理中至少一项处理，包括：

划分步骤，用来将该输入包划分为 B1 位的数据块；

加密处理步骤，用来对这些划分后的 B1 位的数据块执行加密处理或解密处理；

数据块累计步骤，用来累计这些加密数据块，并且在这些数据块的累计值达到 B2 位时输出这些数据块，其中 $B2 = n \times B1$，n 是正整数；

鉴认处理步骤，用来与该加密处理或解密处理并行地对这些输出的 B2

位数据块执行鉴认处理，而且输出标志该鉴认处理结果的鉴认值；

包构造步骤，用来接收这些加密的或解密的数据块，接收该鉴认值，而且构造包括这些接收到的数据块以及该鉴认值的包；

控制步骤，用来判断该输入包是哪一种类型，即，是需要该加密处理与该鉴认处理的第一类型的包、需要该解密处理与该鉴认处理的第二类型的包、只需要该加密处理与该解密处理中的一项处理的第三类型的包或者是只需要该鉴认处理的第四类型的包，以及，如果被判定为该第一类型的包，那么就进行控制以便执行该划分步骤中的划分、该加密处理步骤中的加密处理、该数据块累计步骤中的累计、该鉴认处理步骤中的鉴认处理以及该包构造步骤中的构造。

注意，本发明也可以作为安全通信包处理方法来实现，在这些方法中，上述安全通信包处理装置的典型控制单元就是处理步骤，或者作为使一台计算机执行这些处理步骤的程序。当然，该程序可以通过一种记录媒体（譬如 CD-ROM）或者一种传输媒体（譬如一个通信网络）来进行分配。

附图说明

通过结合为解释本发明的特定实施例所附的附图而作的说明，本发明的这些与其他的目的、优点与特点将会变得显而易见。在这些附图中：

图 1 是一幅流程图，它说明既需要加密处理又需要鉴认处理的包的一个传统处理程序。

图 2 是一幅方框图，它表示符合本发明的第一实施例的安全通信包处理装置的一种结构。

图 3 是一幅示意图，它描述一个加密及鉴认处理控制单元中的数据通道控制。

图 4A 是一幅方框图，它表示加密处理单元的详细结构的一个示例。

图 4B 是一幅示意图，它说明图 4A 所示的一个块加密单元中的加密（或解密）处理的一个示例。

图 5A 是说明数据块累计单元的功能的一幅数据流图。

图 5B 是说明该数据块累计单元中处理程序的一幅流程图。

图 6A 是一幅方框图，它表示鉴认处理单元的详细结构的一个示例。

图 6B 是一幅方框图，它说明图 6A 所示的散列电路中的散列处理的一个概貌。

图 7 是一幅示意图，它说明该加密处理单元中的加密处理以及该鉴认处理单元中的鉴认处理的运行时间安排。

图 8 是一幅示意图，它表示符合本发明的第一实施例的安全通信包处理装置产品的一个应用示例。

图 9A 是说明图 8 所示的安全网关的一幅功能方框图。

图 9B 表示一个说明该安全网关通信功能的协议栈。

图 10 是一幅方框图，它说明符合本发明的第二实施例的安全通信包处理装置的结构。

图 11 是说明该安全通信包处理装置的运行程序的一幅流程图。

图 12 是一幅方框图，它说明符合本发明的第三实施例的安全通信包处理装置的结构。

图 13 是说明该安全通信包处理单元的运行程序的一幅流程图。

图 14 是一幅方框图，它说明符合本发明的第四实施例的安全通信包处理装置的结构。

图 15 是说明该安全通信包处理装置的运行程序的一幅流程图。

图 16 是一幅方框图，它说明符合本发明的第五实施例的安全通信包处理装置的结构。

图 17 是说明该安全通信包处理装置的运行程序的一幅流程图。

图 18 是作为变化形式示例的安全通信包处理装置的一幅方框图。

具体实施方式

下面是参考附图所作的本发明的实施例的说明。

首先解释符合本发明的第一实施例的安全通信包处理装置。

图 2 是说明符合本发明的第一实施例的安全通信包处理装置 100 的一幅方框图。符合该第一实施例的安全通信包处理装置 100 按照一个方框单元来执行对一个包（譬如一个输入的 IP 包）的加密（或解密）处理与鉴认处理、将它重新构造成一个包并将它输出。安全通信包处理装置 100 的特点是，它具有只通过一次包重新构造处理就能既完成加密（包括解密）处理、又完成鉴认处理的必须的基本结构，而且该装置包括以固定方式连接的四个电路块，即一个加密及鉴认处理控制单元 101、一个加密处理单元 102、一个数据块累计单元 103、一个鉴认处理单元 104 以及一个包构造单元 105。

注意，根据这个实施例，被输入到加密及鉴认处理控制单元 101 的包按照应当对这些包执行的处理类型被划分为四类。第一类是一个既需要加密处理又需要鉴认处理的包（一个发送包），第二类是一个既需要解密处理又需要鉴认处理的包（一个接收包），第三类是一个需要加密处理或解密处理的包，而第四类是一个只需要鉴认处理的包。

加密及鉴认处理控制单元 101 从外部接收一个应当进行处理的包以及处理该包所需的信息（下文将称为“处理信息”），而且根据该处理信息执

行对其他部件 102～105 的控制（即控制它们来运行 ON/OFF 等等）以及确定数据通道的控制。此外，它将一个包划分为 B1 位（譬如 64 位）长度的、供加密处理（或解密处理）的数据块来作为加密处理单元 102 的一个处理单元，以便将它们连同它们的处理信息一道输出到加密处理单元 102，而且将一个包划分为 B2 位（譬如 512 位）长度的、供鉴认处理的数据块来作为鉴认处理单元 104 的一个处理单元，以便将它们连同它们的处理信息一道输出到鉴认处理单元 104。

这里的“处理信息”包括是否需要执行加密处理、是否需要执行鉴认处理以及执行何种处理：是加密处理还是鉴认处理。如果需要执行加密处理，那么它包括算法、密钥信息以及 IV（初始向量），而如果需要执行鉴认处理，那么就包括算法、必要的密钥信息以及一个鉴认值。注意，密码算法包括 DES（数据加密标准）与 3DES。同样，鉴认算法包括 HMAC-MD5-96 与 HMAC-SHA-1-96。此外，由于一个包与它的处理信息根据一个识别号码等等彼此对应，所以当多个包被顺序输入到加密及鉴认处理控制单元 101 时，要保证有一个机制使它们不会被混淆。

图 3 是一幅描述加密及鉴认处理控制单元 101 中数据通道控制的示意图。当加密及鉴认处理控制单元 101 根据该处理信息认定相应的包是一个上述第一类型的发送包时，就是说，这个包是一个既需要加密处理又需要鉴认处理的包时，它就分别控制部件 102～105，以便形成一个图 3 中数据通道图 111 所示的数据流。换句话说，对该包以一个数据块为单元顺序执行由加密处理单元 102 进行的加密处理以及由鉴认处理单元 104 进行的鉴认处理，而且鉴认处理的结果（该鉴认值）被输入到包构造单元 105，同时由加密处理单元 102 进行的加密处理结果也被输入到包构造单元 105。

同样，当加密及鉴认处理控制单元 101 认定包是一个上述第二类型的接收包时，就是说，这个包是一个既需要解密处理又需要鉴认处理的包时，它就分别控制部件 102～105，以便形成一个图 3 中数据通道图 112 所示的数据流。换句话说，对该包以一个数据块为单元并行执行由加密处理单元 102 进行的解密处理以及由鉴认处理单元 104 进行的鉴认处理，而且这些结果（即该解密数据块及该鉴认值）被输入到包构造单元 105。

同样，当加密及鉴认处理控制单元 101 认定包是属于该第三类型时，就是说，这个包是一个需要加密处理或解密处理的包时，它就分别控制部件 102～105，以便形成一个图 3 中数据通道图 113 所示的数据流。换句话说，对该包以一个数据块为单元并行执行由加密处理单元 102 进行的加密处理或解密处理以及由鉴认处理单元 104 进行的鉴认处理，而且这些结果（即该加密或该解密数据块以及该鉴认值）被输入到包构造单元 105。

此外，当加密及鉴认处理控制单元 101 认定包是属于该第四类型时，就是说，这个包是一个只需要鉴认处理的包时，它就分别控制部件 102～105，以便形成一个图 3 中数据通道图 114 所示的数据流。换句话说，该包被转送到包构造单元 105，同时对该包以一个数据块为单元执行由鉴认处理单元 104 进行的鉴认处理，而且该结果（即该鉴认值）被输入到包构造单元 105。

加密处理单元 102 是根据加密算法（譬如一个 DES 与 3DES）执行块加密与解密的一个电路或类似器件，它按照一个预定数目的步骤（一个时钟循环）对一个从加密及鉴认处理控制单元 101 发送来的、供 B1 位加密（或解密）处理的数据块执行加密处理，并且将该结果作为加密（或解密）数据块输出到数据块累计单元 103 或包构造单元 105。

图4A是一幅方框图，它说明加密处理单元102的详细结构的一个示例。加密处理单元102包括一个输入块缓冲器121，它存储一个供B1位加密（或解密）处理的输入数据块；一个块加密单元122，它执行该块加密（与解密）以及该块加密（与解密）处理所需的密钥处理；以及一个输出块缓冲器123，它存储该加密（或解密）处理的结果，即存储B1位的加密（或解密）数据块。

图4B是一幅示意图，它说明图4A所示的块加密单元122中的加密（或解密）处理的一个示例。对一个从输入块缓冲器121输出的B1位数据块，执行一个固定的位置换（初始置换），然后执行由密钥确定的16轮加扰处理，最后执行固定的位置换（最终置换）。在执行了用以产生一个调度密钥的处理之后，包含在加密及鉴认处理控制单元101的输出处理信息中的K1位密钥被划分为16个K2位的局部密钥，而且被用来与每个相应的加扰处理中的一个数据块进行一次“异或”运算，并被用来确定位置换的处理细节。

数据块累计单元103是一个队列缓冲器或类似器件，它累计从加密处理单元102输出的加密数据块，并在该累计值达到可以由鉴认处理单元104执行鉴认处理的B2位数据块大小时，将该B2位数据作为一个供鉴认处理的数据块输出到鉴认处理单元104。

图5是一幅表示数据块累计单元103的功能的数据流图。这里，输入到鉴认处理块104的、供鉴认处理的数据块的位长度B2是从加密处理单元102输出的加密数据块的位长度B1的n倍。图5B是表示数据块累计单元103的处理程序的一幅流程图。举例来说，以带有一个指针的B1位宽的寄存器文件来实现的数据块累计单元103重复如下处理（步骤131～134）：复

位该计数器（步骤 131），累计从加密处理单元 102 输出的加密数据块（步骤 132 与 133），而且在这些数据块的数量达到 n 时（步骤 133）将 n 个加密数据块作为 B2 位并行数据输出到鉴认处理单元 104（步骤 134）。

鉴认处理单元 104 是一个根据鉴认算法（譬如 HMAC-MD5-96 与 HMAC-SHA-1-96 等）来执行鉴认处理的电路或类似器件，该鉴认处理包括计算 ICV（完整性检查值）以及确认它的完整性，该鉴认处理单元对从加密及鉴认处理控制单元 101 或者从数据块累计单元 103 输出的、从供鉴认处理的 B2 位数据块按照预定数目的步骤（一个时钟循环）执行鉴认处理，而且将该结果作为该鉴认值输出到包构造单元 105。

图 6A 是一幅方框图，它表示鉴认处理单元 104 的详细结构的一个示例。鉴认处理单元 104 包括一个输入块缓冲器 141，它存储一个供该鉴认处理的 B2 位输入数据块；一个散列电路 142，它为供鉴认处理的 m 个数据块计算一个 A 位（譬如说 96 位）散列值，该散列值通过对从输入块缓冲器 141 发送的、供鉴认处理的数据块执行散列处理而构成一个包；以及一个鉴认值输出缓冲器 143，它将该计算所得的散列值存储为鉴认值。

图 6B 是一幅示意图，它表示图 6A 所示散列电路 142 的散列处理的概貌。输入到输入块缓冲器 141 的 B2 位数据块按照根据当时由散列电路 142 存储的 A1 位鉴认值所确定的方法加以处理，以便修改该 A1 位鉴认值。接着，输入的 B2 位数据块按照根据刚刚修改的 A1 位鉴认值确定的方法加以处理，以便进一步修改由散列电路 142 存储的 A1 位鉴认值。重复这一过程，而且将对上一个 B2 位数据块修改的 A1 位散列值的一部分用来作为这个包的 A2 位鉴认值。

包构造单元 105 按照符合从加密及鉴认处理控制单元 101 获悉的处理

信息或类似信息的顺序来排列从加密处理单元 102 输出的这些加密（或解密）数据块以便对它们进行累计，而且通过将从鉴认处理单元 104 输出的鉴认值组合到一个预定的位置来构造一个与输入到加密及鉴认处理单元 101 的包对应的、经过处理的包。更具体地讲，对上述第一类型的一个发送包，通过累计从加密处理单元 102 输出的加密数据块并组合从鉴认处理单元 104 输出的鉴认值，重新构造一个具有预定格式的、经过加密及鉴认处理的包。对上述第二类型的一个接收包，通过累计从加密处理单元 102 输出的解密数据块，重新构造一个具有预定格式的、经过解密与鉴认处理的数据块。类似地，对第三类型的包，通过累计从加密处理单元 102 输出的加密（或解密）数据块，重新构造一个具有预定格式的、经过加密（或解密）的包。而对第四类型的包，一个输入到安全通信包处理装置 100 的包被构造成一个符合预定格式的、经过鉴认处理的包。

注意，一个加密数据块的重新构造包括按照与一个隧道模式及一个传送模式对应的格式来重新构造一个由 IPSec 规定的加密有效负载（ESP：封装安全有效负载）。类似地，重新构造一个鉴认值包括按照与一个隧道模式及一个传送模式对应的格式来重新构造一个由 IPSec 规定的鉴认标头（AH：鉴认标头）。举例来说，包括的包类型有 Ipv4 与 Ipv6。

下面，将按照输入上述四类包的情形来分别说明符合这个实施例的、根据上述方式构造的安全通信包处理装置 100 的运行情况。

首先说明向安全通信包处理装置 100 输入第一类包的情形，即输入一个既需要加密处理又需要鉴认处理的包的情形（相应于图 3 中数据通道图 111 的处理过程）。

作为第一步骤，加密及鉴认处理控制单元 101 接收一个应当被处理的

包及其处理信息。加密及鉴认处理控制单元 101 根据该处理信息判定该包是一个既需要加密处理又需要鉴认处理的发送包，将该包划分为供加密处理的数据块，而且将它们连同其处理信息一道发送到加密处理单元 102。

作为第二步骤，加密处理单元 102 接收从加密及鉴认处理控制单元 101 输出的处理信息以及供加密处理的数据块，根据该处理信息确定应当被应用到该数据块的一个加密算法、一个密钥、一个 IV 以及一个加密处理方法，而且按照该加密方法对这些供加密处理的数据块进行加密。注意，它的实现方法可以是在加密处理单元 102 中处理多个加密算法。将这些加密数据块输出到包构造单元 105，并同时将它们与鉴认处理所必须的处理信息一道输出到数据块累计单元 103 以便进行随后的鉴认处理。注意，加密处理单元 102 在每次输入下一个供加密处理的数据块时重复执行该处理过程。

作为第三步骤，数据累计单元 103 不断累计从加密处理单元 102 输出的供加密处理的数据块，直到它们达到鉴认处理所必须的数据块大小为止，而且当它们达到该鉴认处理所必须的数据块大小时，它将它们连同其处理信息一道输出到鉴认处理单元 104。数据块累计单元 103 利用数据块累计单元 103 具有的一个累计块计数器或类似器件来计数以便判断累计状态，即这些加密数据块的累计值是否等于供鉴认的数据块大小。注意，这可以通过使加密及鉴认处理控制单元 101 包含该累计块计数器的方法来实现。

数据块累计单元 103 在每次输入下一个加密数据块时累计该数据块，重复判断这些数据块的数目是否达到 n 块，而且在它到达 n 时向鉴认处理单元 104 输出这些累计的数据块。

作为第四步骤，鉴认处理单元 104 从数据块累计单元 103 接收这些供鉴认处理的加密数据块及其处理信息，根据该处理信息执行该鉴认处理，

而且计算该鉴认值。鉴认处理单元 104 的输出值是当前正在被处理的包的鉴认值。

上述第一至第四步骤被重复应用于既需要加密处理又需要鉴认处理的发送包中既需要加密处理又需要鉴认处理的所有数据块。

最后，作为第五步骤，包构造单元 105 按照预定的顺序排列从加密处理单元 102 输出的加密数据块以便对它们进行累计，并将从鉴认处理单元 104 输出的该鉴认值组合到一个预定的位置来构造一个与输入到加密及鉴认处理控制单元 101 的包对应的、经过加密及鉴认处理的包。

图 7 是一幅示意图，它表示加密处理单元 102 中的加密处理与鉴认处理单元 104 中的鉴认处理的运行时间安排。这里，一个包被划分为 m×n 个供加密处理的数据块，而且 n 个供加密处理的数据块（加密数据块）对应于一个供鉴认处理的数据块。所以，一个包被划分为 m 个供鉴认处理的数据块。

如图 7 所示，在加密处理单元 102 中执行了加密处理的加密数据块在数据块累计单元 103 中被逐个累计。当 n 个加密数据块在数据块累计单元 103 中被累计时，这种加密数据块中有 n 块被从数据块累计单元 103 中取出，并被传送到鉴认处理单元 104，在那里它们被作为供鉴认处理的第一个数据块接收鉴认处理。按照这种方法，该加密处理与该鉴认处理并行重复进行。结果，对这一个发送包执行 m× n 次加密处理，但只执行 m 次鉴认处理。注意，由于输入到安全通信包处理装置 100 的发送包的长度、加密与鉴认算法以及其他情况并不固定，所以加密处理与鉴认处理的次数可以根据伴随该包的处理信息动态确定。

下面说明向安全通信包处理装置 100 输入第二类包的情形，即输入一

个既需要解密处理又需要鉴认处理的接收包的情形（相应于图 3 中数据通道图 112 的处理过程）。

作为第一步骤，加密及鉴认处理控制单元 101 接收一个应当被处理的包及其处理信息。加密及鉴认处理控制单元 101 根据该处理信息判定该包是一个既需要解密处理又需要鉴认处理的接收包。然后，它将一个包划分为供解密处理的数据块来作为一个供解密处理的包，并将它们连同其处理信息一道输出到加密处理单元 102，而且将另一个包划分为供鉴认处理的数据块来作为一个供鉴认处理的包，并将它们连同其处理信息一道输出到鉴认处理单元 104。

作为第二步骤，如下两类处理被并行执行。该第一类处理是，加密处理单元 102 根据这些接收到的数据块的处理信息对它们进行解密，并将它们输出到包构造单元 105。该第二类处理是，鉴认处理单元 104 对接收到的供鉴认处理的数据块执行鉴认处理，并计算该鉴认值。

上述第一与第二步骤被重复应用于既需要解密处理又需要鉴认处理的接收包中既需要解密处理又需要鉴认处理的所有数据块。

最后，作为第三步骤，包构造单元 105 根据加密及鉴认处理控制单元 101 提供的信息、按照预定的顺序排列从加密处理单元 102 输出的解密数据块以便对它们进行累计，而且它将鉴认处理单元 104 输出的鉴认值组合到一个预定的位置，以便构造一个与输入到加密及鉴认处理控制单元 101 的包对应的、经过解密与鉴认处理的包。

下面详细说明向安全通信包处理装置 100 输入第三类包的情形，即输入一个需要加密处理或者需要解密处理的包的情形（相应于图 3 中数据通道图 113 的处理过程）。

作为第一步骤，加密及鉴认处理控制单元 101 接收一个应当被处理的包及其处理信息。加密及鉴认处理控制单元 101 根据该处理信息判定该包是一个需要加密处理或者需要解密处理的包，将它划分为供加密处理的数据块，而且将它们连同其处理信息一道输出到加密处理单元 102。

作为第二步骤，加密处理单元 102 接收这些供加密处理的数据块及其处理信息，根据该处理信息执行加密处理或解密处理，并且将它们作为已经处理的数据块输出到包构造单元 105。

上述第一与第二步骤被重复应用于需要加密处理或者需要解密处理的包中需要加密处理或者需要解密处理的所有数据块。

最后，作为第三步骤，包构造单元 105 根据加密及鉴认处理控制单元 101 提供的信息、按照预定的顺序排列从加密处理单元 102 输出的加密（或解密）数据块以便对它们进行累计，而且它构造一个与输入到加密及鉴认处理控制单元 101 的包对应的、经过加密（或解密）处理的包。

下面说明向安全通信包处理装置 100 输入第四类包的情形，即输入一个只需要鉴认处理的包的情形（相应于图 3 中数据通道图 114 的处理过程）。

作为第一步骤，加密及鉴认处理控制单元 101 接收一个应当被处理的包及其处理信息。加密及鉴认处理控制单元 101 根据该处理信息判定该包是一个只需要鉴认处理的包，将它划分为供鉴认处理的数据块，而且将它们连同其处理信息一道输出到鉴认处理单元 104。

作为第二步骤，鉴认处理单元 104 接收这些供鉴认处理的数据块及其处理信息，根据该处理信息执行该鉴认处理，并且计算该鉴认值。

上述第一与第二步骤被重复应用于仅需要鉴认处理的包中需要鉴认处理的所有数据块。

最后，作为第三步骤，包构造单元 105 根据加密及鉴认处理控制单元 101 提供的信息将从鉴认处理单元 104 输出的鉴认值组合到已经输入到安全通信包处理装置 100 的包，以便构造一个与输入到加密及鉴认处理控制单元 101 的包对应的、经过鉴认处理的包。

如上所述，根据本发明的安全通信包处理装置 100，一个输入到安全通信包处理装置 100 的包被判定属于四类包中的哪种类型，被划分为所需大小的数据块，而且接收加密（或解密）与鉴认，以便通过仅仅一次包重新构造过程来恢复成为一个经过处理的包。

换句话说，传统上，首先对一个既需要加密处理又需要鉴认处理的包执行加密处理来将它构造成为一个加密包，然后再将它划分为需要加以鉴认的供鉴认处理的数据块，所以该包需要在加密处理与鉴认处理后进行两次构造，而且鉴认处理单元 104 必须等到这些加密数据块被重新构造成一个包为止。而另一方面，根据这个实施例，在加密处理单元 102 与鉴认处理单元 104 之间提供了数据块累计单元 103，所以，总是能将大小为处理所必须而且足供处理的数据块输入到加密处理单元 102 与鉴认处理单元 104，而且对任何安全处理只需要重新构造该划分后的包一次即可。就是说，由于数据块累计单元 103 累计加密数据块，直到它们达到供鉴认处理必须的数据块大小为止，而且将它们输出到鉴认处理单元 104，所以与传统方法相比，鉴认处理单元 104 的输入等待时间大为降低。相应地，对该包的安全处理的处理能力得以改进、延迟得以降低、处理速度得以加快，而且该加密处理单元与该鉴认处理单元的有效利用也成为可能。

图 8 是一幅示意图，它说明符合本发明的第一实施例的安全通信包处理装置产品的一个示例。这里图解说明了作为一个路由器与一座防火墙的

安全网关 160 的外形。安全网关 160 是一个通信装置，它能安全地连接作为一个公共通信网络的 WAN 161（譬如互联网）与作为连接室内使用的多台计算机及其他设备的一个专用通信网络的 LAN 162。更具体地可以举例来讲，这个安全网关 160 是一个位于 IP 层次的网关，它与按照 IETF（互联网工程任务队）出版的注释 2401～2410 的要求而公布的 IPSec 规范相对应。对一个从 LAN 162 向 WAN 161 输出的 IP 包，可以根据需要执行加密处理与鉴认处理、只执行加密处理或者只执行鉴认处理，而对一个从 WAN 161 向 LAN 161 输出的 IP 包，可以执行解密处理与鉴认处理、只执行解密处理或者只执行鉴认处理，从而通过一条能够消除欺诈行为（譬如第三方的侦听或伪装）的安全通信通道经由 WAN 161 来连接多个通信装置。

图 9A 是说明图 8 所示安全网关 160 的结构的一幅功能方框图，而图 9B 表示一个说明安全网关 160 的通信功能的协议栈。安全网关 160 包括本实施例的安全通信包处理装置 100，它通过一个 LSI 或类似器件来实现；一个 WAN 接口 165，它是连接到 WAN 161 的通信接口；一个 LAN 接口 166，它是连接到 LAN 162 的通信接口；以及一个网络控制器 167，它根据图 9B 所示协议栈经由这两个接口 165 与 166 来转换输入与输出的数据，并且控制安全通信包处理装置 100 来对一个 IP 包执行加密（或解密）处理与鉴认处理。

这个安全网关 160 加快了经由互联网的安全通信。举例来说，需要实时通信、交互通信（譬如一项电子结算）以及发布数字作品（譬如一幅活动图像）的一个互联网电话的通信速度与安全性都能得到显著的改进。

注意，根据这个实施例的安全通信包处理装置 100，在加密及鉴认处理单元 101 的控制下可以确定并管理每个部件之间的数据传输以及一个数据

通道，但是举例来说，不采用这种方法或者除此之外，也可以采用每个处理单元之间的双向握手方法来实现加密及鉴认处理控制单元 101、加密处理单元 102、数据块累计单元 103 与鉴认处理单元 104 之间的数据传输。

而且，这个实施例的安全通信包处理装置 100 可以采用一个 LSI 以及一个 FPGA（现场可编程门阵列）来实现，或者，加密处理单元 102 与鉴认处理单元 104 可以采用一个 DSP（数字信号处理器）来实现。

此外，尽管在这个实施例中，数据块累计单元 103 独立于鉴认处理单元 104，但是本发明并不总是局限于这一结构，而且数据块累计单元 103 可以采用被包含在鉴认处理单元 104 之内的方法来实现。

下面说明符合本发明的第二实施例的安全通信包处理装置。

图 10 是一幅方框图，它说明符合本发明的第二实施例的安全通信包处理装置 200 的结构。这个实施例的安全通信包处理装置 200 是具有两个或两个以上加密处理单元与/或鉴认处理单元、而且数据块累计单元数量与加密处理单元数量相同的装置的一个示例。这里，该第二实施例具有的一种结构是，一对由一个加密处理单元、一个数据块累计单元与一个鉴认处理单元构成的组合（下文称为“一个包处理模块”）平行排列，就是说，这种结构相当于两个符合该第一实施例的安全通信包处理装置 100 的单元。更具体地讲，安全通信包处理装置 200 包括内含一个加密处理单元 202a、一个数据块累计单元 203a、一个鉴认处理单元 203a 与一个包构造单元 205a 的包处理模块；内含一个加密处理单元 202b、一个数据块累计单元 203b、一个鉴认处理单元 204b 与一个包构造单元 205b 的包处理模块；以及一个加密及鉴认处理控制单元 201。

注意，加密处理单元 202a 与 202b、数据块累计单元 203a 与 203b、鉴

认处理单元204a与204b以及包构造单元205a与205b分别与符合该第一实施例的加密处理单元102、数据块累计单元103、鉴认处理单元104以及包构造单元105具有相同的功能。此外，ID号被分别分配到加密处理单元202a与202b、鉴认处理单元204a与204b以及数据块累计单元203a与203b中以便对它们进行惟一识别。下面说明该第二实施例，特别是它与该第一实施例的不同点。

除了该第一实施例的加密及鉴认处理单元101的功能之外，加密及鉴认处理控制单元201还具有有效利用两对包处理模块来作为资源的控制功能。更具体地讲，加密及鉴认处理控制单元201始终跟踪处理状态，譬如各个处理单元202a～205a与202b～205b是否在执行处理（BUSY），或者是否准备就绪进行处理（READY），跟踪方法是从各个处理单元接收标志它们正在执行处理的BUSY信号或标志它们已准备就绪进行处理的READY信号。这里，当两个加密处理单元202a与202b都准备就绪进行处理时，具有最低ID号的加密处理单元被优先使用。当两个鉴认处理单元同时准备就绪进行处理时，也采用同样的规则。

不过，举例来说，当在加密处理单元202b中对一个既需要加密处理又需要鉴认处理的传送包执行加密处理时，加密及鉴认处理控制单元201就进行控制，使得从加密处理单元202b输出的加密数据块在数据块累计单元203b中累计之后被输入到鉴认处理单元204b，而且在包构造单元205b中重新进行构造。就是说，对既需要加密处理又需要鉴认处理的一个发送包，对它进行处理的数据块累计单元、鉴认处理单元以及包构造单元根据执行该处理的加密处理单元自行确定。总之，一个包的加密（或解密）处理、数据块的累计、鉴认处理以及重新构造由同一个包处理模块内的处理单元

执行。

图 11 是说明安全通信包处理装置 200 的运行程序的一幅流程图。当加密及鉴认处理控制单元 201 接收到一个需要加密处理、需要鉴认处理或者两者都需要的包及其处理信息时，如果该包需要加密处理，它就指定已经准备就绪进行处理的加密处理单元 202a 或 202b，并将该包（划分后的数据块）及其处理信息输出到加密处理单元 202a 或 202b。另一方面，如果该包只需要鉴认处理时，那么加密及鉴认处理控制单元 201 就指定已经准备就绪进行处理的鉴认处理单元 204a 或 204b，并将该包（划分后的数据块）及其处理信息输出到鉴认处理单元 204a 或 204b（步骤 211）。随后的加密（或解密）处理以及鉴认处理按照该第一实施例中所述的方法执行，即按照根据一个包的类型来确定的程序以及四类数据通道中的一条来执行。

如上所述，根据这个实施例的安全通信包处理装置 200，提供了两个或两个以上的加密处理单元与/或鉴认处理单元，多个包被该加密及鉴认处理控制单元分配到处于空闲状态的加密处理单元或鉴认处理单元，而且该加密处理与鉴认处理对这多个包并行进行。所以，将多个需要加密处理或鉴认处理的包顺序输入到一个单独的处于“准备就绪进行处理”状态的包处理模块并造成传输迟延的问题得以避免，从而安全通信的传输速度也得以改善。

注意，尽管根据这个实施例说明了一对包含一个加密处理单元、一个鉴认处理单元以及一个数据块累计单元的组合被并行排列的一种结构，但是本发明并不总是局限于上述结构，而且也可以实现一种提供若干加密处理单元与鉴认处理单元以使这些加密处理单元的处理性能总和等于这些鉴认处理单元的处理性能总和的结构。在这种情况下，加密处理单元与鉴认

处理单元的数量之比可以根据加密处理单元数量：鉴 认处理单元数量＝ n T1：T2 来计算，当一个供加密处理的数据块大小为 B1，一个供鉴认处理的数据块大小是 B2 （＝ n B 1）时，加密处理单元中每一块的处理步骤数是 T1，而鉴认处理单元中每一块的处理步骤数是 T2。注意，B、n、T1 与 T2 都是自然数。

下面说明符合本发明的第三实施例的安全通信包处理装置。

图 12 是一幅方框图，它说明符合本发明的第三实施例的安全通信包处理装置 300 的一种结构。这个实施例的安全通信包处理装置 300 是具有多个加密处理单元、多个数据块累计单元以及多个鉴认处理单元，其连接方式不固定且可以动态确定的装置的一个示例。它包括一个加密及鉴认处理控制单元 301、一个数据通道连接切换单元 302、两个加密处理单元 303a 与 303b、两个数据块累计单元 304a 与 304b、两个鉴认处理单元 305a 与 305b 以及一个包构造单元 306。

注意，加密处理单元 303a 与 303b、数据块累计单元 304a 与 304b、鉴认处理单元 305a 与 305b 以及包构造单元 306 与符合该第一实施例的加密处理单元 102、数据块累计单元 103、鉴认处理单元 104 以及包构造单元 105 具有相同的功能。此外，ID 号被分别分配到加密处理单元 303a 与 303b、鉴认处理单元 305a 与 305b 以及数据块累计单元 304a 与 304b 中以便对它们进行惟一识别。下面说明该第三实施例，特别是它与该第一实施例的不同点。

数据通道连接单元 302 是一个选择器电路或类似电路，它可以根据加密及鉴认处理控制单元 301 的控制来分别并且独立地连接（或维持不连接）加密及鉴认处理控制单元 301 的输出与加密处理单元 303a 或 303b 的输入、

加密及鉴认处理控制单元 301 的输出与鉴认处理单元 305a 或 305b 的输入、加密处理单元 303a 的输出与数据块累计单元 304a 或 304b 的输入、加密处理单元 303b 的输出与数据块累计单元 304a 或 304b 的输入、数据块累计单元 304a 的输出与鉴认处理单元 305a 或 305b 的输入、数据块累计单元 304b 的输出与鉴认处理单元 305a 或 305b 的输入。

除了该第一实施例的加密及鉴认处理控制单元 101 的功能之外，加密及鉴认处理控制单元 301 还具有控制数据通道切换单元 302，使得各个部件中只有必要的部件被动态连接，以便有效地利用六个部件 303a、303b、304a、304b、305a 与 305b 作为资源的功能。

图 13 是说明安全通信包处理单元 300 的一种运行程序的一幅流程图。加密及鉴认处理控制单元 301 从外部接收一个应当被处理的包及其处理信息，判断该包的一个类型，即根据该处理信息的内容判断需要进行加密（或解密）处理与鉴认处理，而且指定能够执行必要处理的（或者准备就绪进行处理的）加密处理单元 303a 或 303b、数据块累计单元 304a 或 304b 以及鉴认处理单元 305a 或 305b（步骤 311）。

然后，加密及鉴认处理控制单元 301 向数据通道连接切换单元 302 发出一个连接命令，使得每个指定的处理单元按照由它的包类型决定的方式进行连接（步骤 312）。这里，“连接命令”可以由每个需要连接的处理单元的一个 ID 号来表示，或者类似于选择器的一个控制信号。如果判定该包是一个第一类型的发送包，那么加密及鉴认处理控制单元 301 就向数据通道连接切换单元 302 发出一个连接加密及鉴认处理控制单元 301 的输出与加密处理单元 303b 的输入的命令、一个连接加密处理单元 303b 的输出与数据块累计单元 304b 的输入的命令以及一个连接数据块累计单元 304b 的输

出与鉴认处理单元 305b 的输入的命令。

另一方面，当该连接完成时，数据通道连接切换单元 302 将一个表明该连接已经完成的 READY 信号输出到加密及鉴认处理控制单元 301（步骤 313）。

当加密及鉴认处理控制单元 301 接收到一个 READY 信号时，它就将该需要处理的包划分为处理所需的数据块，并且将它们连同其处理信息一道经由数据通道连接切换单元 302 输出到每个处理单元 303a、303b、305a 与 305b。从而，根据该第一实施例中描述的处理程序来执行必要的加密（或解密）处理、必要的鉴认处理以及该包的重新构造（步骤 314）。

下面按照每种包类型来说明在该第一实施例中描述的四类包被输入到安全通信包处理装置 300 时的详细运行情况。

首先，解释一个第一类包，即一个既需要加密处理又需要鉴认处理的发送包被输入到安全通信包处理装置 300 时的处理过程。作为第一步骤，加密及鉴认处理控制单元 301 接收一个需要处理的包及其处理信息，根据该处理信息的内容判定这是一个既需要加密处理又需要鉴认处理的发送包，而且按照该第二实施例中描述的方法判定哪些加密单元、数据块累计单元以及鉴认处理单元已经准备就绪进行处理。

这里，举例来说，当加密处理单元 303b、数据块累计单元 304b 与鉴认处理单元 305b 已经准备就绪进行处理时，作为第二步骤，加密及鉴认处理单元 301 就向数据通道连接切换单元 302 发出一个连接加密及鉴认处理控制单元 301 的输出与加密处理单元 303b 的输入的命令、一个连接加密处理单元 303b 的输出与数据块累计单元 304b 的输入的命令以及一个连接数据块累计单元 304b 的输出与鉴认处理单元 305b 的输入的命令。

另一方面，作为第三步骤，数据通道连接切换单元 302 根据该给定的连接命令来连接各个处理单元，并且在完成该连接后，它将一个标志连接成功的 READY 信号输出到加密及鉴认处理控制单元 301。

作为第四步骤，当加密及鉴认处理控制单元 301 从数据通道连接切换单元 302 接收到该 READY 信号时，它将该包划分为供加密处理的数据块，并且将它们连同其处理信息一道输出到加密处理单元 303b。随后的处理按照用于该第一实施例中描述的一个第一类型发送包的处理方法执行。

其次，解释一个第二类包，即一个既需要解密处理又需要鉴认处理的接收包被输入到安全通信包处理装置 300 时的处理过程。作为第一步骤，加密及鉴认处理控制单元 301 接收一个需要处理的包及其处理信息，根据该处理信息的内容判定这是一个既需要解密处理又需要鉴认处理的接收包，而且判定哪些解密处理单元以及鉴认处理单元已经准备就绪进行处理。

这里，举例来说，当加密处理单元 303b 与鉴认处理单元 305b 已经准备就绪进行处理时，作为第二步骤，加密及鉴认处理单元 301 就向数据通道连接切换单元 302 发出一个连接加密及鉴认处理控制单元 301 的输出与加密处理单元 303b 的输入的命令以及一个连接加密及鉴认处理控制单元 301 的输出与鉴认处理单元 305b 的输入的命令。

作为第三步骤，数据通道连接切换单元 302 根据该给定的连接命令来连接加密及鉴认处理控制单元 301 与加密处理单元 303b，连接加密及鉴认处理控制单元 301 与鉴认处理单元 305b，并且在完成该连接后，它将一个 READY 信号输出到加密及鉴认处理控制单元 301。

作为第四步骤，加密及鉴认处理控制单元 301 按照与该第一实施例中所描述的相同方法复制该包，将一个包划分为供加密处理的数据块以便将

它们输出到加密处理单元 303b，而且将另一个包划分为供鉴认处理的数据块以便将它们输出到鉴认处理单元 305b。随后的处理按照用于该第一实施例中描述的一个第二类包的处理方法执行。

下面，解释一个第三类包，即一个既需要加密处理又需要鉴认处理的包被输入到安全通信包处理装置 300 时的处理过程。作为第一步骤，加密及鉴认处理控制单元 301 接收一个需要处理的包及其处理信息，根据该处理信息的内容判定这是一个需要加密处理或解密处理的包，而且判定哪个处理单元已经准备就绪进行处理。

这里，举例来说，当加密处理单元 303b 已经准备就绪进行处理时，作为第二步骤，加密及鉴认处理单元 301 就向数据通道连接切换单元 302 发出一个连接加密及鉴认处理控制单元 301 的输出与加密处理单元 303b 的输入的命令。

作为第三步骤，数据通道连接切换单元 302 根据该给定的连接命令来连接加密及鉴认处理控制单元 301 与加密处理单元 303b，而且在完成该连接之后，它将一个 READY 信号输出到加密及鉴认处理控制单元 301。

作为第四步骤，加密及鉴认处理控制单元 301 将该包划分为供加密处理的数据块以便将它们输出到加密处理单元 303b。随后的处理按照用于该第一实施例中描述的一个第三类包的处理方法执行。

最后，解释一个第四类包，即一个需要鉴认处理的包被输入到安全通信包处理装置 300 时的处理过程。作为第一步骤，加密及鉴认处理控制单元 301 接收一个需要处理的包及其处理信息，根据该处理信息的内容判定这是一个需要鉴认处理的包，而且判定哪个鉴认处理单元已经准备就绪进行处理。

这里，举例来说，当鉴认处理单元 305b 已经准备就绪进行处理时，作为第二步骤，加密及鉴认处理单元 301 就向数据通道连接切换单元 302 发出一个连接加密及鉴认处理控制单元 301 的输出与鉴认处理单元 305b 的输入的命令。

作为第三步骤，数据通道连接切换单元 302 根据该给定的连接命令来连接加密及鉴认处理控制单元 301 与鉴认处理单元 305b，而且在完成该连接之后，它将一个 READY 信号输出到加密及鉴认处理控制单元 301。

作为第四步骤，加密及鉴认处理控制单元 301 将该包划分为供加密处理的数据块以便将它们输出到鉴认处理单元 305b。随后的处理按照用于该第一实施例中描述的一个第四类包的处理方法执行。

如上所述，根据符合这个实施例的安全通信包处理装置 300，因为由一个加密处理单元、一个数据块累计单元以及一个鉴认处理单元构成的一个集合并非总是被固定占用，所以通过提供数据通道连接切换单元 302 来经由各种通道连接各个处理单元，就实现了灵活的结构，使得一个加密处理单元能够将数据块输入到任意一个已经准备就绪进行处理的数据块累计单元，而且一个数据块累计单元能够将数据块输入到任意一个已经准备就绪进行处理的鉴认处理单元。就是说，由于该加密处理单元、该数据块累计单元以及该鉴认处理单元能够被灵活组合，所以它们能够被有效地利用。此外，提供多个加密处理单元与鉴认处理单元，或者用安装了另一个加密算法的加密处理单元来替换安装了加密算法的加密处理单元，就能很容易地实现这类运行方式。

下面说明符合本发明的第四实施例的安全通信包处理装置。

图 14 是一幅方框图，它说明符合本发明的第四实施例的安全通信包处

理装置 400 的结构。符合该第四实施例的安全通信包处理装置 400 包括这样一种结构，即在符合该第三实施例的安全通信包处理装置 300 上附加六个分别连接到两个加密处理单元、两个数据块累计单元以及两个鉴认处理单元的保存区域（或者处理数据保存单元）。换句话说，安全通信包处理装置 400 包括一个加密及鉴认处理控制单元 401，一个数据通道连接切换单元 402，两个加密处理单元 403a 与 403b，两个数据块累计单元 404a 与 404b，两个鉴认处理单元 405a 与 405b，六个处理数据保存单元 406a、406b、406c、406d、406e 与 406f，以及一个包构造单元 407。下面说明该第四实施例，特别是它与该第三实施例的不同点。

六个处理数据保存单元 406a、406b、406c、406d、406e 与 406f 是存储器或类似器件，它们具有仅供分别暂时保存正在相应的加密处理单元 403a 与 403b、数据块累计单元 404a 与 404b 以及鉴认处理单元 405a 与 405b 中处理的所有数据的存储区域。

注意，尽管根据该第四实施例，加密及鉴认处理控制单元 401 接收在该第一实施例中描述的四种类型的包及其处理信息，但是可以设想该处理信息包括关于处理这些包的优先级信息。举例来说，“关于优先级的信息”可以用数字表示。譬如说，这些数字按照 IP 标头中所包含的服务类型（ToS）位的信息来分配。

除了加密及鉴认处理控制单元 301 的功能外，加密及鉴认处理控制单元 401 还根据该输入包的优先级来执行分配资源（就是说，加密处理单元、数据块累计单元与鉴认处理单元）的处理。更具体地讲，如果加密（或解密）处理与鉴认处理需要的所有资源在该包输入时都已被占用，那么加密及鉴认处理控制单元 401 就在它们之中指定处理具有最低优先级的包的资

源，并将其处理数据保存在处理数据保存单元以便释放该资源。换句话说，加密及鉴认处理控制单元 401 执行控制使得具有最高优先级的包被较早处理。

图 15 是说明安全通信包处理装置 400 的运行程序的一幅流程图。

加密及鉴认处理控制单元 401 接收一个需要处理的包及其处理信息，然后根据该处理信息判断处理该包所需的处理单元是否准备就绪进行处理（步骤 411）。结果，当该所需处理单元已经准备就绪进行处理时（步骤 411 中的“Yes”），加密及鉴认处理控制单元 401 就将这些数据块及其处理信息输出到该处理单元，并且随后使它执行与该第三实施例中的处理过程（图 13 的步骤 311～314）相应的处理（步骤 412）。

另一方面，当处理该包需要的所有处理单元都被占用时（步骤 411 中的“No”），加密及鉴认处理控制单元 401 就给处理具有最低优先级的包的处理单元发出一个将处理中途的数据保存到与该处理单元连接的处理数据保存单元的命令（步骤 413）。当该处理单元接收到该保存命令时，它将处理中途的数据及其处理信息保存到处理数据保存单元，而且在完成该保存后，它将一个 READY 信号输出到加密及鉴认处理控制单元 401（步骤 414）。

当加密及鉴认处理控制单元 401 接收到该 READY 信号时，它将数据块及其处理信息输出到该处理单元，并且随后使它执行与该第三实施例中的处理过程（图 13 的步骤 311～314）相应的处理（步骤 415）。在所有对该包按照优先级进行的处理完成之后，该处理单元从该处理数据保存单元读出处理中途的数据，并重新开始对该包进行处理（步骤 416）。

如上所述，根据该第四实施例的安全通信包处理装置 400，除了该第三实施例的结构之外，还提供了处理数据保存单元 406a、406b、406c、406d、

406e 与 406f。所以，除了在该第三实施例中描述的效果之外，还能够按照优先级来控制对包的处理。

注意，尽管对所有加密处理单元、数据块累计单元与鉴认处理单元分别提供了这些处理数据保存单元，但本发明并不总是局限于上述结构。举例来说，也可以只对所有加密处理单元提供这些处理数据保存单元，就是说，可以对任意处理单元分别提供这些处理数据保存单元。而且，这个实施例可以应用于符合该第二实施例的安全通信包处理装置 200。这种情况下的处理可以按照与上述方法相同的方法来实现。

此外，根据这个实施例，如果所有需要的处理单元在一个包被输入到加密及鉴认处理控制单元 301 时都被占用，那么正在处理各个包中具有最低优先级的包的处理单元就不管该输入包的优先级而在处理中途被强制释放，但是，也可以附加与该输入包的优先级的相关性来作为一个释放条件。可以举例来说，正在处理优先级比该输入包优先级更低、而且在各个包中具有最低优先级的包的处理单元可以在处理中途被强制释放。

此外，不仅是一个包的优先级，而且一个包的大小、处理所需的步骤数、要完成这些处于处理中途的包的处理还需要的步骤数等等也可以被用来作为确定该处理单元的一个参数。

下面说明符合本发明的第五实施例的安全通信包处理装置。

图 16 是一幅示意图，它说明符合本发明的第五实施例的安全通信包处理装置 500 的结构。符合该第五实施例的安全通信包处理装置 500 包括这样一种结构，即在符合该第二实施例的安全通信包处理装置 200 上附加由两个加密处理单元、两个数据块累计单元以及两个鉴认处理单元共享的一个数据保存区域（一个处理数据保存单元）。换句话说，安全通信包处理装

置 500 包括由一个加密处理单元 502a、一个数据块累计单元 503a、一个鉴认处理单元 504a 以及一个包构造单元 506a 构成的包处理模块，由一个加密处理单元 502b、一个数据块累计单元 503b、一个鉴认处理单元 504b 以及一个包构造单元506b构成的包处理模块，一个加密及鉴认处理控制单元501以及一个处理数据保存单元 505。

处理数据保存单元 505 是一个存储器或类似器件，它被连接到加密处理单元 502a 与 502b、数据块累计单元 503a 与 503b 以及鉴认处理单元 504a 与 504b，而且具有仅供暂时保存这些处理单元内处理中途的所有数据的一个存储器区域。

注意，尽管根据该第五实施例，加密及鉴认处理控制单元 501 按照与该第四实施例相同的方法接收在该第一实施例中描述的四类包及其处理信息，但是可以设想该处理信息包括关于处理这些包的优先级信息。

除了符合该第二实施例的加密及鉴认处理控制单元 201 的功能外，加密及鉴认处理控制单元 501 还根据该输入包的优先级来执行分配资源（包处理模块）的处理。更具体地讲，如果该加密（或解密）处理与鉴认处理需要的所有资源在该包输入时都被占用，那么加密及鉴认处理控制单元 501 就在它们之中指定处理具有最低优先级的包的资源，并在处理中途将该数据保存到处理数据保存单元 505 以便释放该资源。换句话说，加密及鉴认处理控制单元 501 执行控制使得具有较高优先级的包被较早处理。

图 17 是说明安全通信包处理装置 500 的运行程序的一幅流程图。首先，加密及鉴认处理控制单元 501 接收一个需要处理的包及其处理信息，然后根据该处理信息判断处理该包所需的处理单元是否准备就绪进行处理（步骤 511）。结果，当该所需处理单元已经准备就绪进行处理时（步骤 511 中

的“Yes”），加密及鉴认处理控制单元 501 就将这些数据块及其处理信息输出到该处理单元，并且随后使它执行与该第二实施例中的处理过程（图 11 的步骤 211～212）相应的处理（步骤 512）。

另一方面，当处理该包需要的所有处理单元都被占用时（步骤 511 中的“No”），加密及鉴认处理控制单元 501 就给正在处理具有最低优先级的包的处理单元发出一个将处理中途的数据连同保存目的地的一个地址一道保存到该处理数据保存单元 505 的命令（步骤 513）。当该处理单元接收到该保存命令时，它将处理中途的数据及其处理信息保存到处理数据保存单元 505 的规定地址，而且在完成该保存后，它将一个 READY 信号输出到加密及鉴认处理控制单元 501（步骤 514）。

当加密及鉴认处理控制单元 501 接收到该 READY 信号时，它将数据块及其处理信息输出到该处理单元，并且随后使它执行与该第二实施例中的处理过程（图 11 的步骤 211～212）相应的处理（步骤 515）。在所有对该包按照优先级进行的处理完成之后或者其他处理单元达到准备就绪进行处理的状态之后，该处理单元从该处理数据保存单元 505 读出处理中途的数据，并重新开始对该包进行处理（步骤 516）。

如上所述，根据该第五实施例的安全通信包处理装置 500，除了该第二实施例的结构之外，还提供了由加密处理单元 502a 与 502b、数据块累计单元 503a 与 503b 以及鉴认处理单元 504a 与 504b 共享的处理数据保存单元 505。所以，除了在该第二实施例中描述的效果之外，不仅能够按照优先级来控制对包的处理，而且还能比对每个处理单元专门提供处理数据保存单元的第四实施例更有效地利用处理数据保存单元。

注意，尽管根据该第五实施例，该处理数据保存单元为所有加密处理

单元、数据块累计单元与鉴认处理单元所公享，但本发明并不总是局限于上述结构。举例来说，也可以只对所有加密处理单元提供该处理数据保存单元，就是说，可以对这些处理单元的任意组合共同提供该处理数据保存单元。

而且，符合该第五实施例的共享数据保存区域的技术可以应用于符合该第三实施例的安全通信包处理装置 300。更具体地讲，像图 18 所示的安全通信包处理装置 600 一样，可以附加由加密处理单元 602a 与 602b、数据块累计单元 603a 与 603b 以及鉴认处理单元 604a 与 604b 共享的一个数据保存区域（一个处理数据保存单元 606）。在这种情况下，一个加密及鉴认处理控制单元 601 向一个数据通道连接切换单元 602 发出一个将该处理单元作为在处理中途保存数据的目的地而与处理数据保存单元 606 加以连接的命令，以便能够保存该数据。

如同本发明的上述五个实施例所示，由于根据本发明，一个既执行加密处理又执行鉴认处理的处理单元是一个大小为处理所必须且足供处理的数据块，所以，与一个处理单元就是一个包的现有技术相比，加密与鉴认处理速度能够加快，而且迟延能够降低。

同样，根据本发明，在既执行加密处理又执行鉴认处理时，加密处理后的数据块被累计到它们达到鉴认处理所必须而且足供处理的数据块大小为止，而且当它们与供鉴认处理的数据块大小相等时，就执行该鉴认处理。所以，本发明能够有助于节省存储器资源以便作为该加密处理后的数据块的缓冲器。

同样，根据本发明，由于提供了两个或两个以上的加密处理单元与/或鉴认处理单元，所以能够同时处理多个包，而且对这些包的安全处理能力

也能够得到改善。

此外，根据本发明，通过提供数据通道连接切换单元，那么即使在具有多个加密处理单元与/或鉴认处理单元的情况下，该加密处理单元、数据块累计单元以及鉴认处理单元也不需要始终相对固定。这就是说，由于在加密处理后需要鉴认处理的数据块可以被输出到任意一个数据块累计单元，而且该数据块累计单元的输出可以被输出到任意一个鉴认处理单元，所以就会获得这样的效果，即能够更加有效地利用该加密处理单元、数据块累计单元与鉴认处理单元，可以很容易地替换该加密处理单元与该鉴认处理单元，而且可以很容易地增加它们的数量。

此外，通过提供该处理数据保存单元，包处理就并不总是要按照输入到该安全通信包处理装置的顺序来执行，而且该处理顺序也可以根据包的优先级以及其他因素来处理。

还有，根据本发明，由于在该处理数据保存单元中存在任何数据块时，共享该处理数据保存单元、而且已经准备就绪进行处理的任意一个加密处理单元或鉴认处理单元都可以处理该需要处理的数据块，所以通过以加密处理单元、鉴认处理单元以及数据块累计单元的任意组合来共享该处理数据保存单元，就能更有效地使用该加密处理单元与该鉴认处理单元。

尽管已经根据五个实施例说明了符合本发明的安全通信包处理单元，但是本发明并不局限于这些实施例。

就是说，通过对这五个实施例的特点进行组合，可以实现其他各种方式的实施例。举例来说，将该第四实施例的特点（即对每个处理单元提供处理数据保存单元）应用到该第二实施例，就能够实现处理数据保存单元被专门连接到图 10 所示安全通信包处理装置 200 的各个处理单元 202a、

202b、203a、203b、204a 与 204b 的安全通信包处理装置。

此外，符合该第二至第五实施例的安全通信包处理装置，也像符合该第一实施例的安全通信包处理装置一样可以被组合到一个通信设备，譬如组合到安全网关以及计算机设备。

工业实用性

符合本发明的安全通信包处理装置适用于一个通信中继站，该中继站连接各种通信网络、用作一个路由器与一座防火墙的一个安全网关以及一个通信设备，该通信设备安全地连接作为公共网络的一个 WAN 与作为连接多台内部使用计算机的非公共网络的一个 LAN。

图1

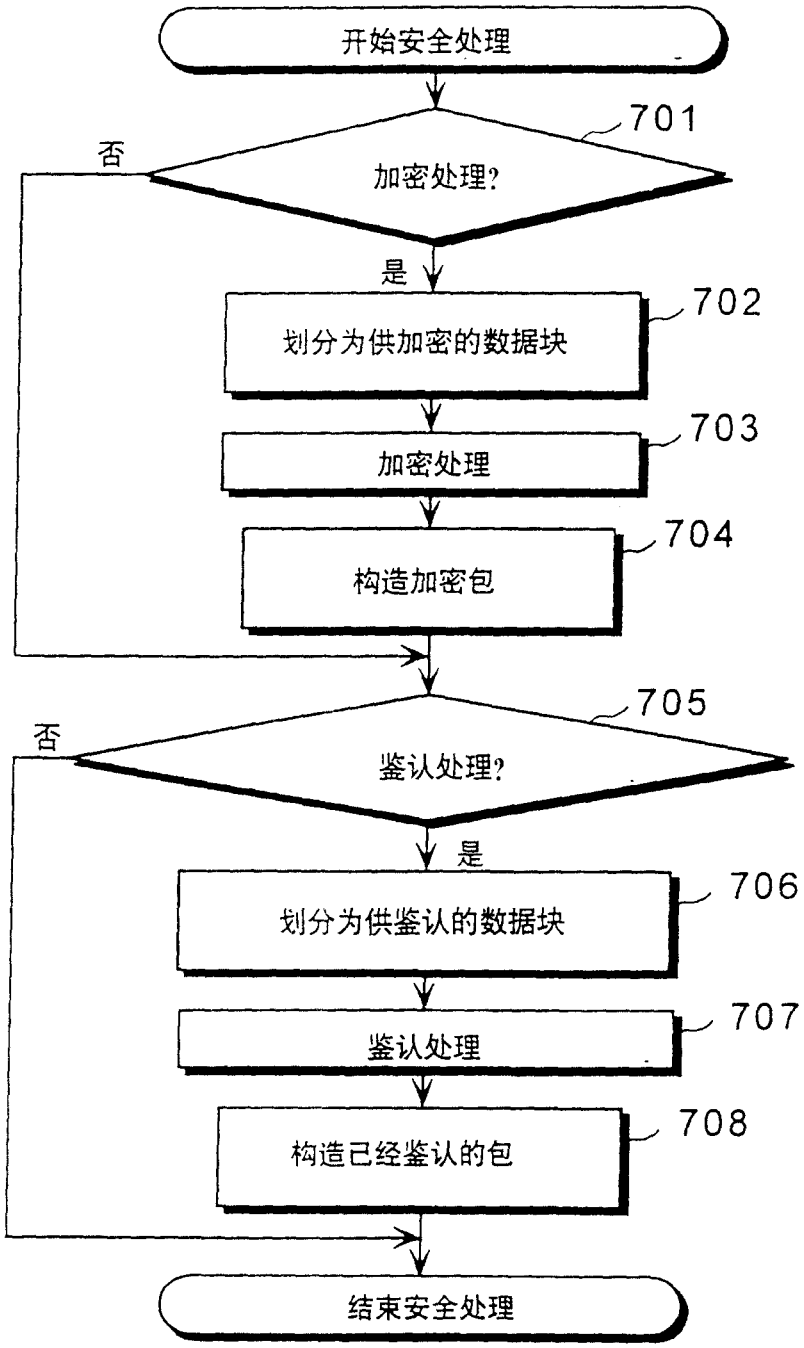

开始安全处理
701
加密处理?
否
是
702
划分为供加密的数据块
703
加密处理
704
构造加密包
705
鉴认处理?
否
是
706
划分为供鉴认的数据块
707
鉴认处理
708
构造已经鉴认的包
结束安全处理

图2

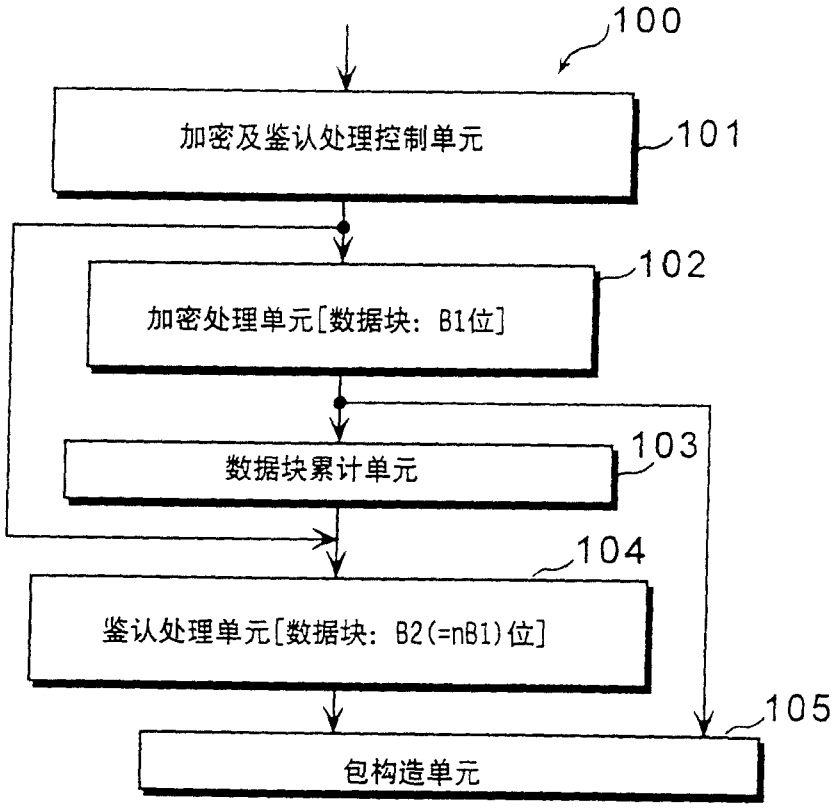

100
加密及鉴认处理控制单元
101
加密处理单元[数据块：B1位]
102
数据块累计单元
103
鉴认处理单元[数据块：B2(=nB1)位]
104
包构造单元
105

图3

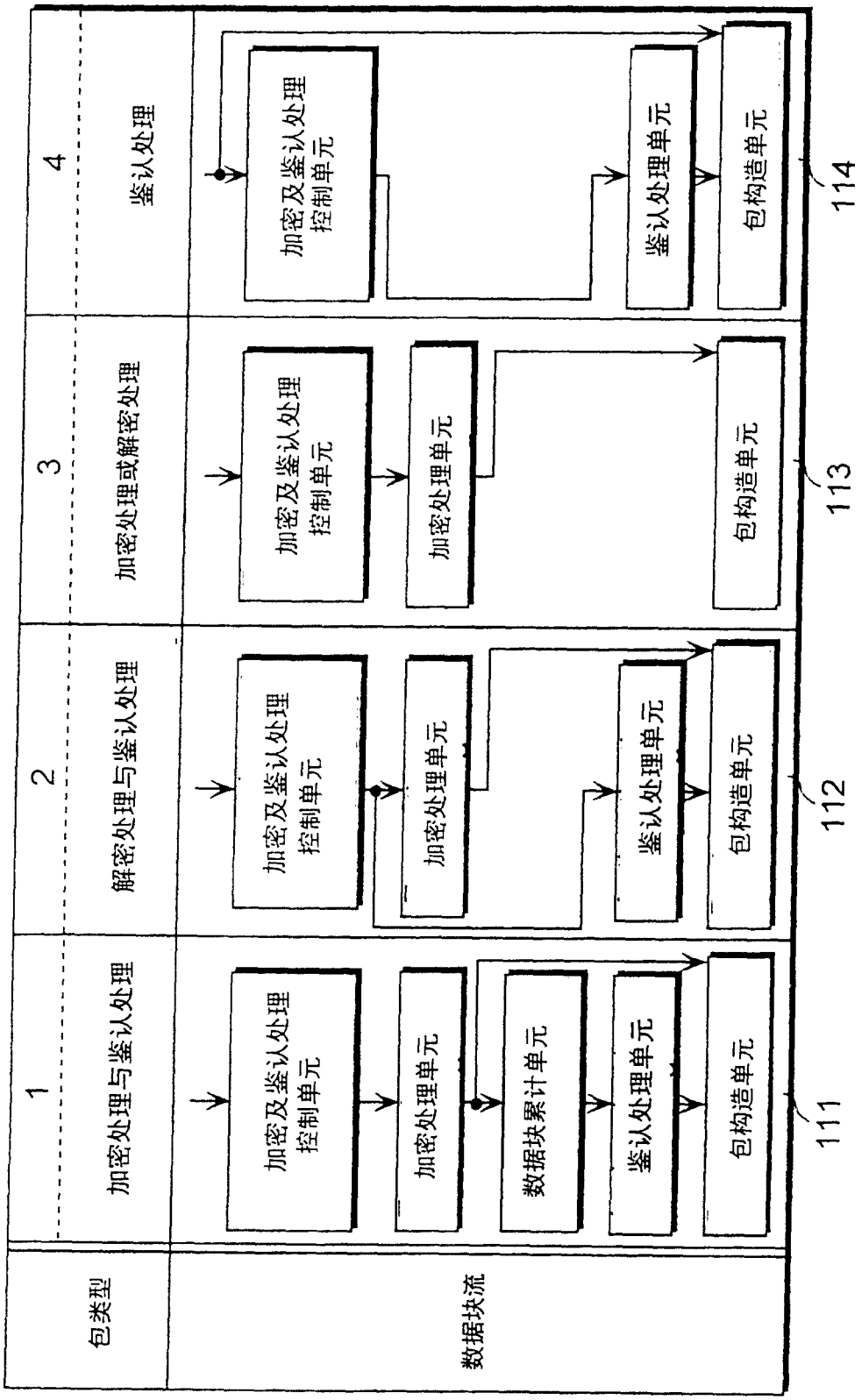

包类型
数据块流
1
加密处理与鉴认处理
2
解密处理与鉴认处理
3
加密处理或解密处理
4
鉴认处理
加密及鉴认处理控制单元
加密处理单元
数据块累计单元
鉴认处理单元
包构造单元
111
112
113
114

图4A

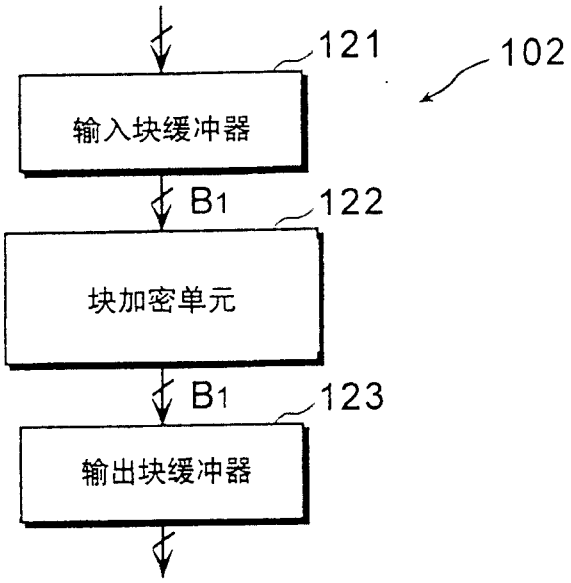

121
102
输入块缓冲器
B1
122
块加密单元
B1
123
输出块缓冲器

图4B

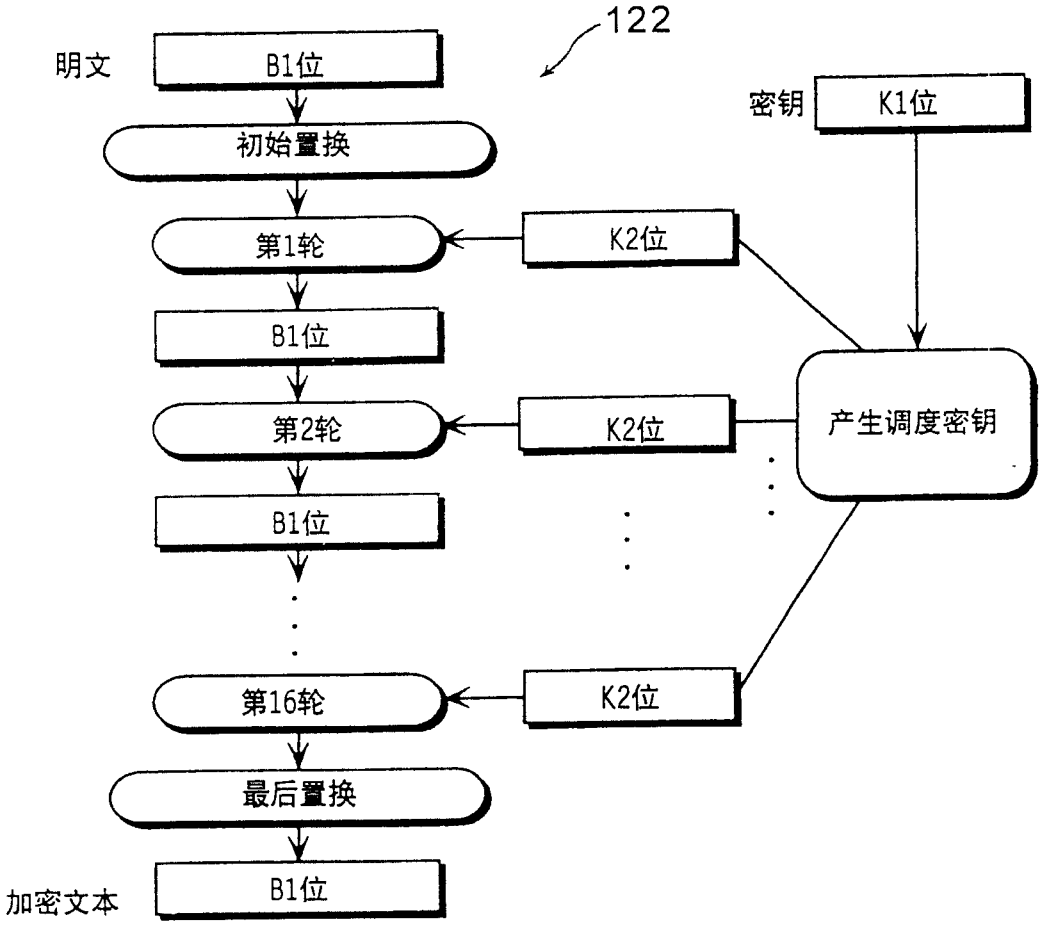

122
明文
B1位
初始置换
第1轮
K2位
B1位
第2轮
K2位
B1位
第16轮
K2位
最后置换
B1位
加密文本
密钥
K1位
产生调度密钥

图5A

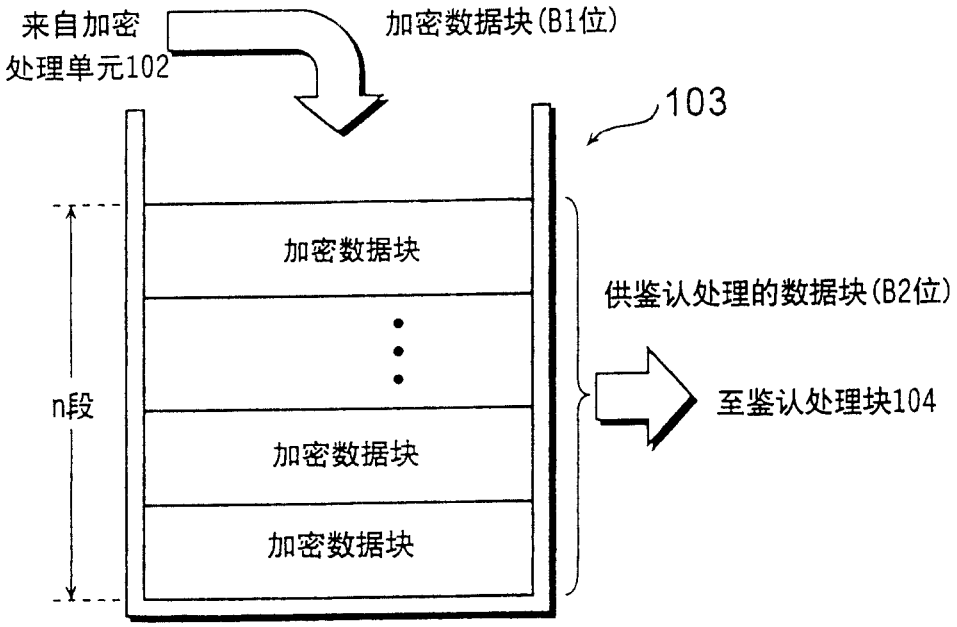

来自加密
处理单元102
加密数据块(B1位)
103
加密数据块
供鉴认处理的数据块(B2位)
n段
至鉴认处理块104
加密数据块
加密数据块

图5B

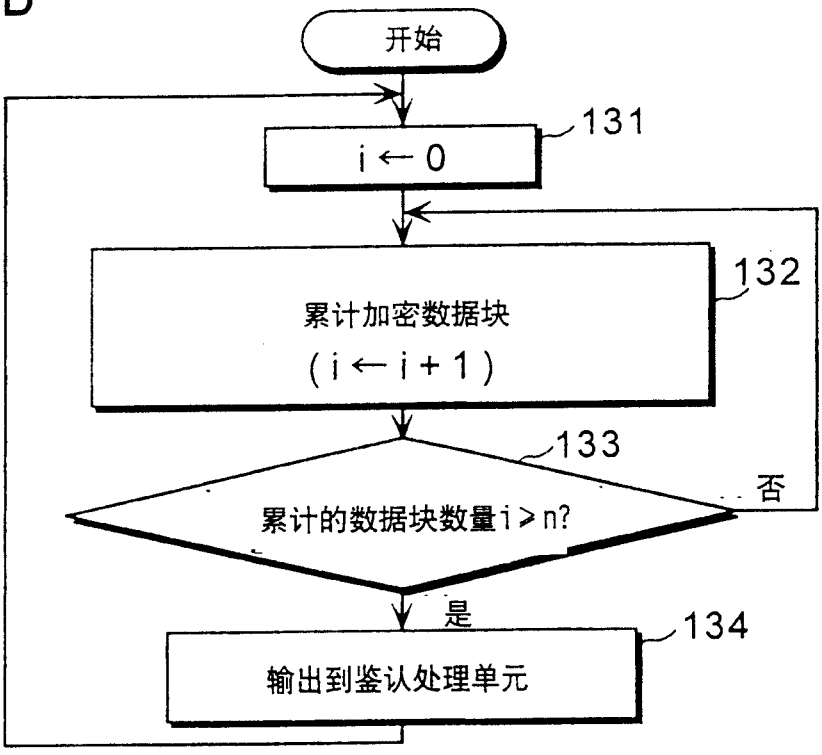

开始
131
i ← 0
132
累计加密数据块
(i ← i + 1)
133
否
累计的数据块数量i ≥ n?
是
134
输出到鉴认处理单元

图6A

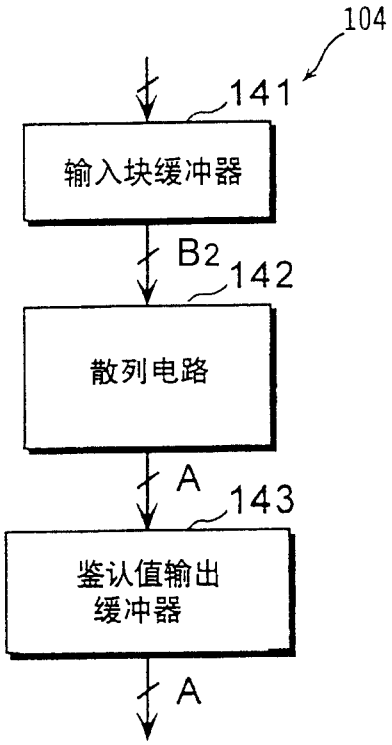

104
141
输入块缓冲器
B2
142
散列电路
A
143
鉴认值输出
缓冲器
A

图6B

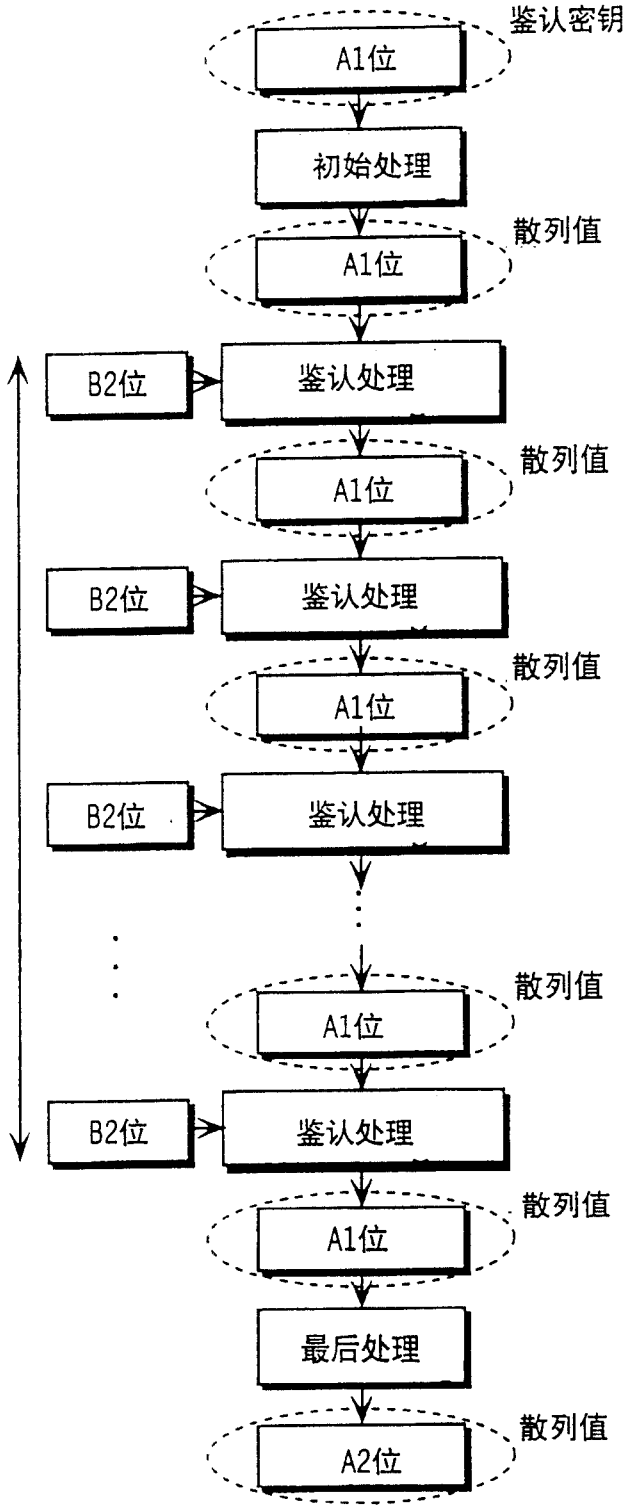

鉴认密钥
A1位
初始处理
散列值
A1位
B2位
鉴认处理
散列值
A1位
B2位
鉴认处理
散列值
A1位
B2位
鉴认处理
散列值
A1位
B2位
鉴认处理
散列值
A1位
最后处理
散列值
A2位

图7

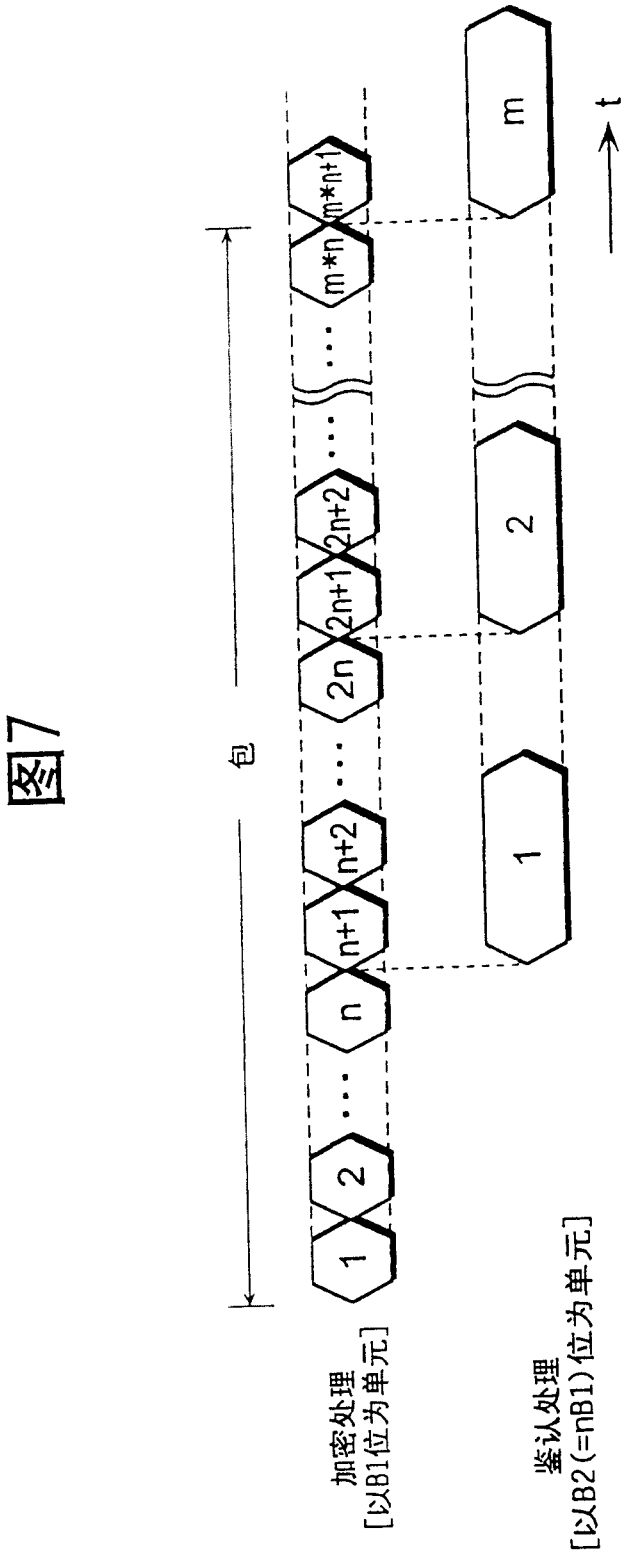


图8

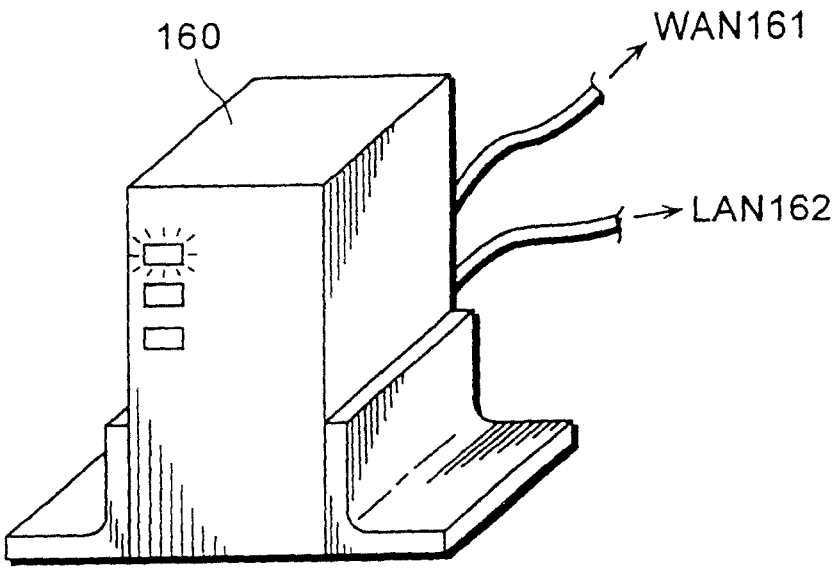


图9A

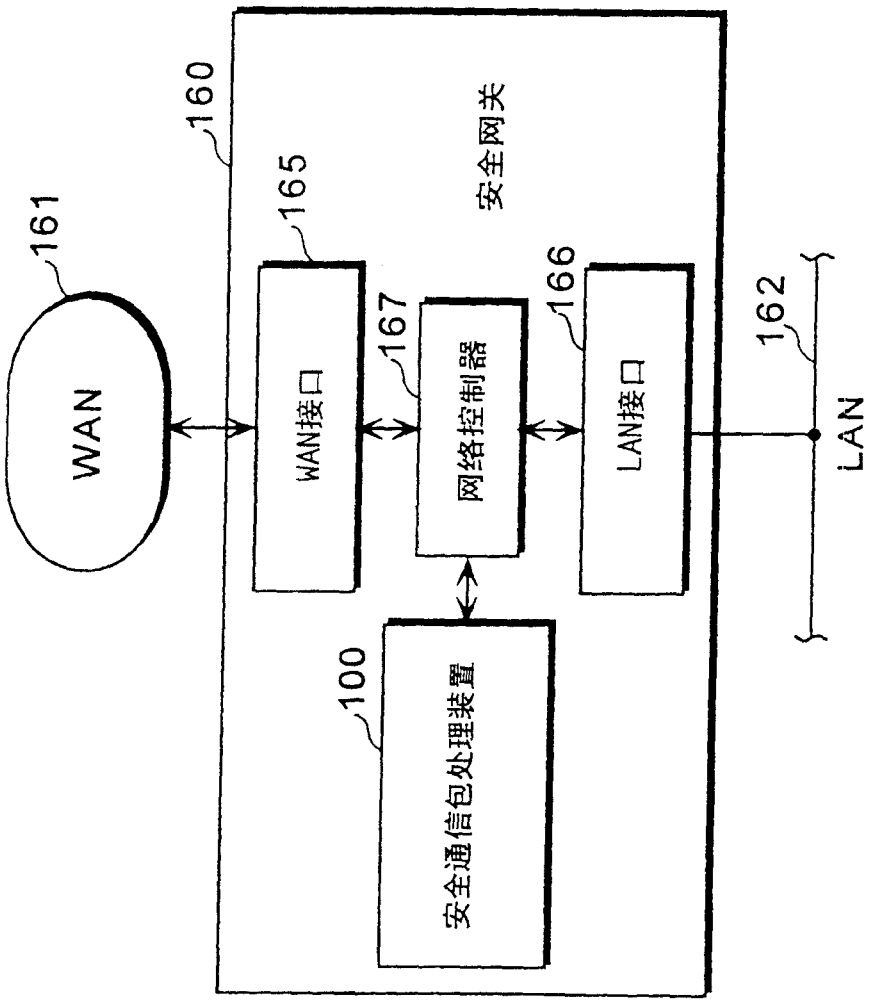

WAN
161
160
安全网关
165
WAN接口
167
网络控制器
166
LAN接口
162
LAN
100
安全通信包处理装置

图9B

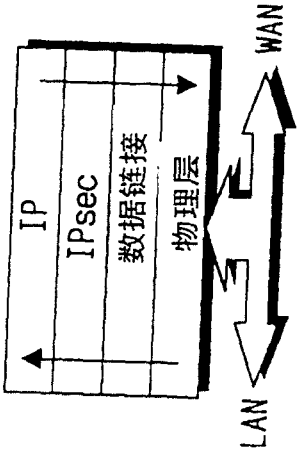

IP
IPsec
数据链接
物理层
WAN
LAN

图10

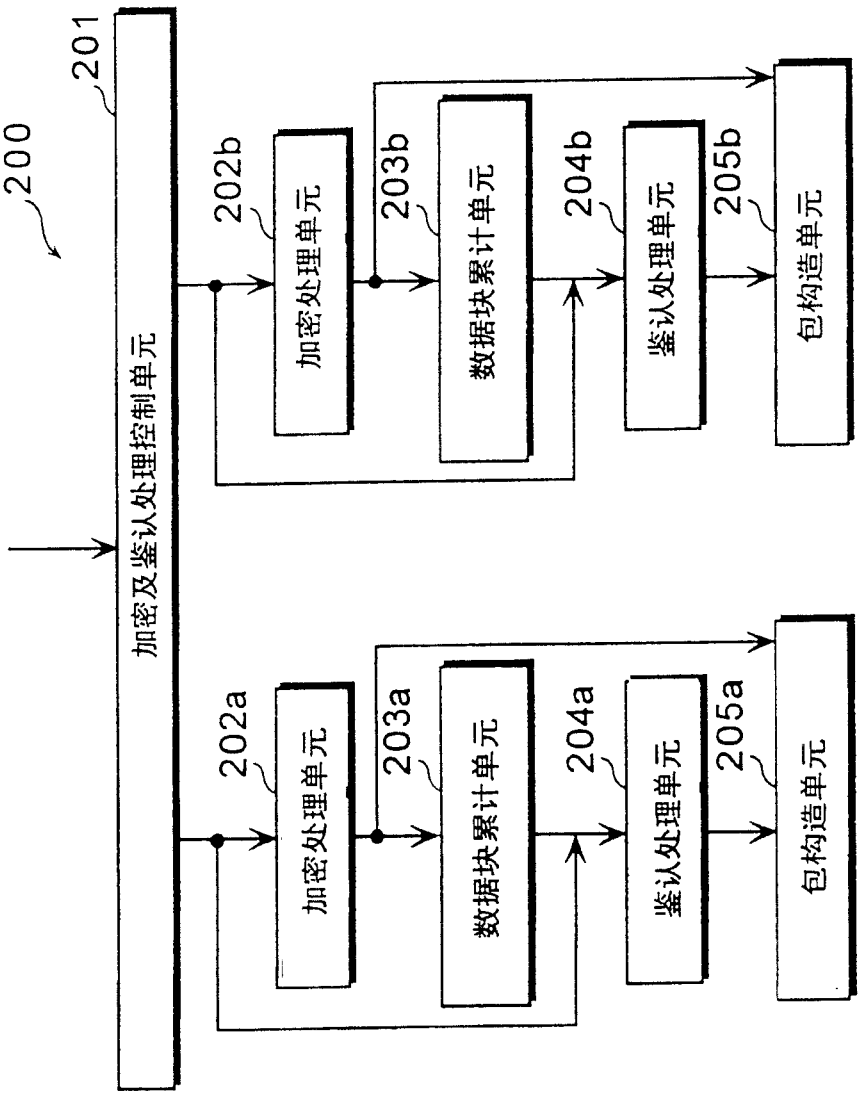

200
201
加密及鉴认处理控制单元
202b
加密处理单元
203b
数据块累计单元
204b
鉴认处理单元
205b
包构造单元
202a
加密处理单元
203a
数据块累计单元
204a
鉴认处理单元
205a
包构造单元

图11

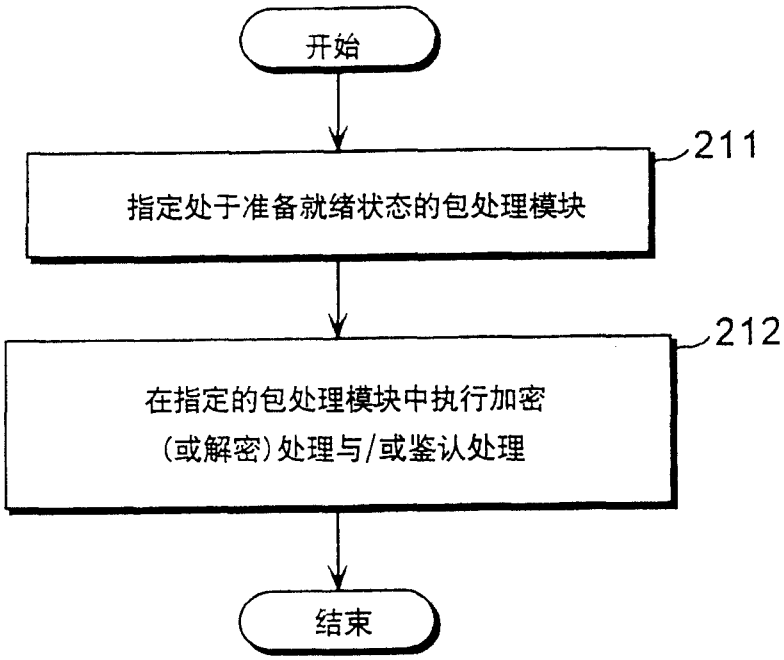

开始
211
指定处于准备就绪状态的包处理模块
212
在指定的包处理模块中执行加密
(或解密)处理与/或鉴认处理
结束

图12

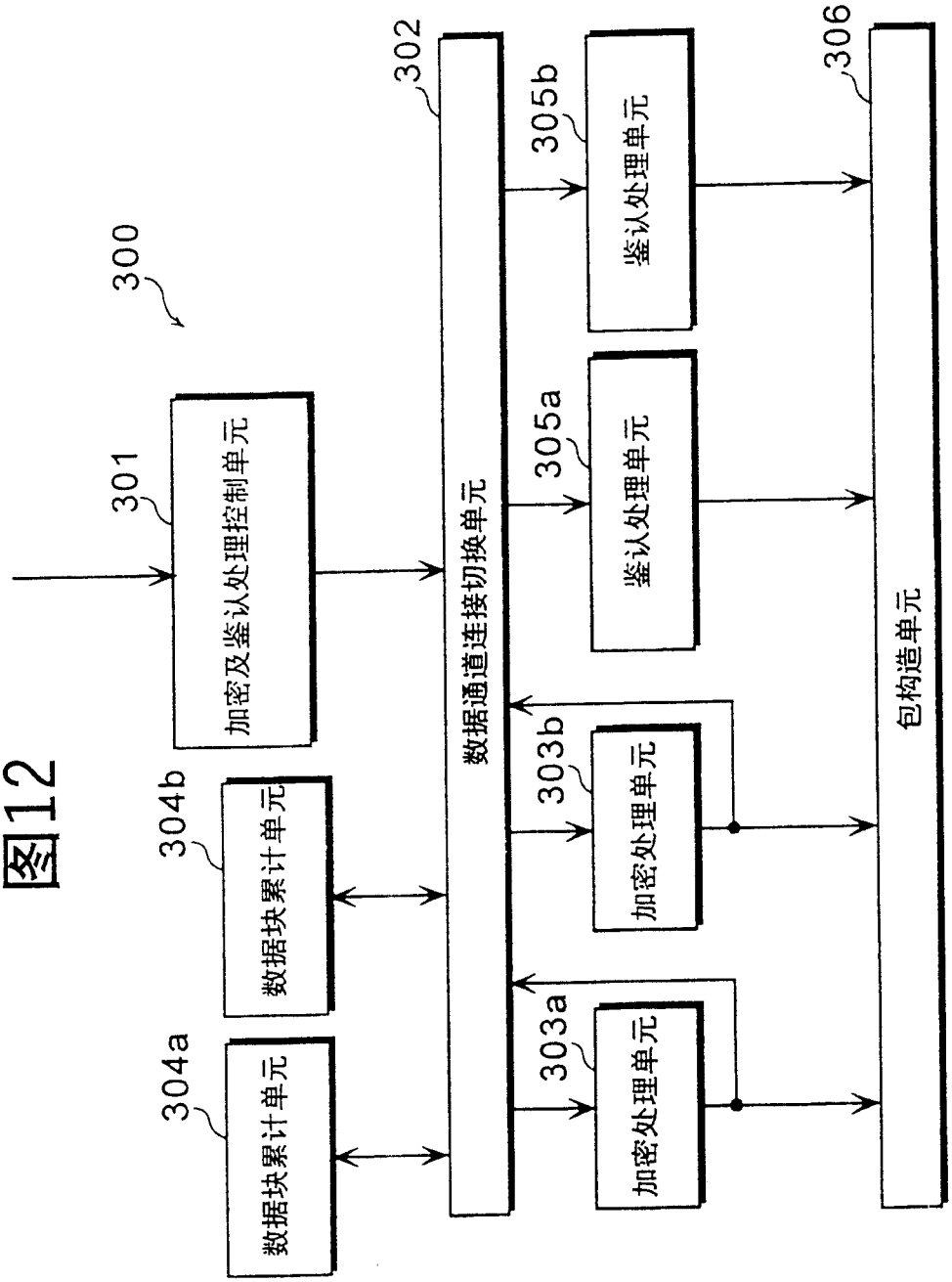

300
301
加密及鉴认处理控制单元
302
数据通道连接切换单元
303a
加密处理单元
303b
加密处理单元
304a
数据块累计单元
304b
数据块累计单元
305a
鉴认处理单元
305b
鉴认处理单元
306
包构造单元

图13

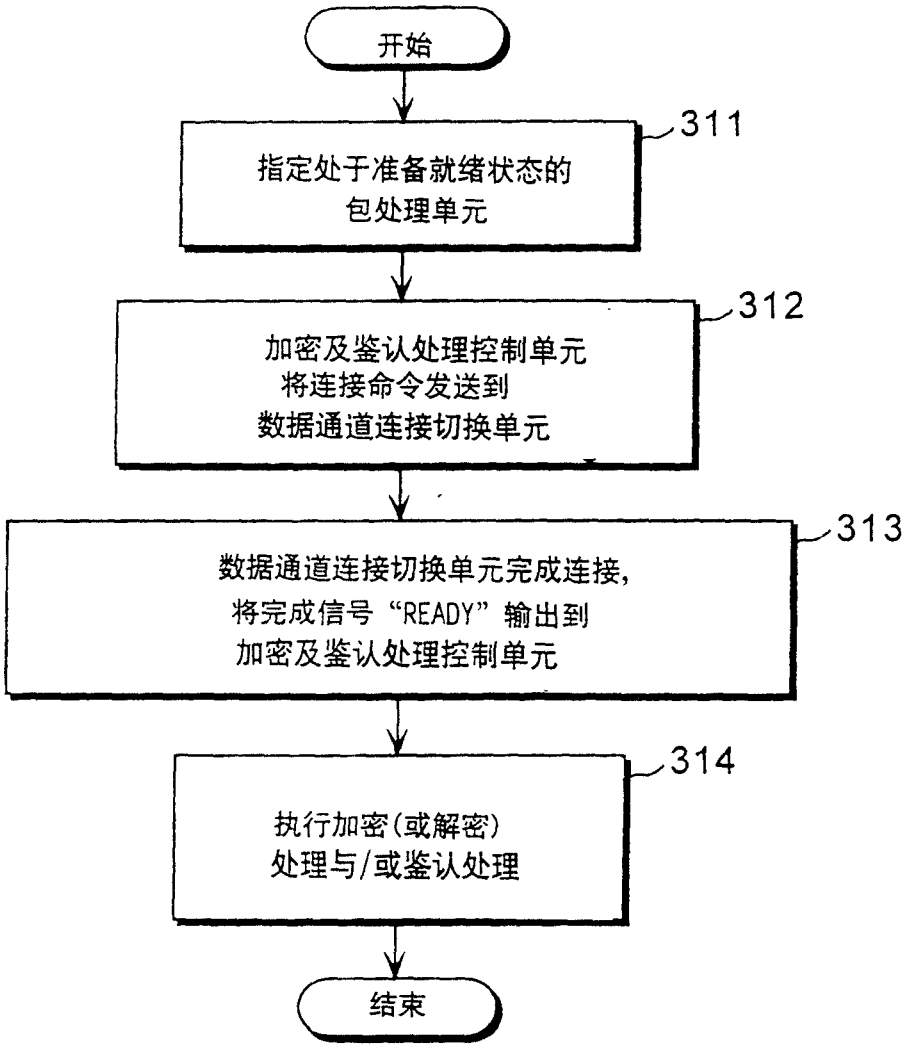

开始
311
指定处于准备就绪状态的
包处理单元
312
加密及鉴认处理控制单元
将连接命令发送到
数据通道连接切换单元
313
数据通道连接切换单元完成连接，
将完成信号“READY”输出到
加密及鉴认处理控制单元
314
执行加密(或解密)
处理与/或鉴认处理
结束

图14

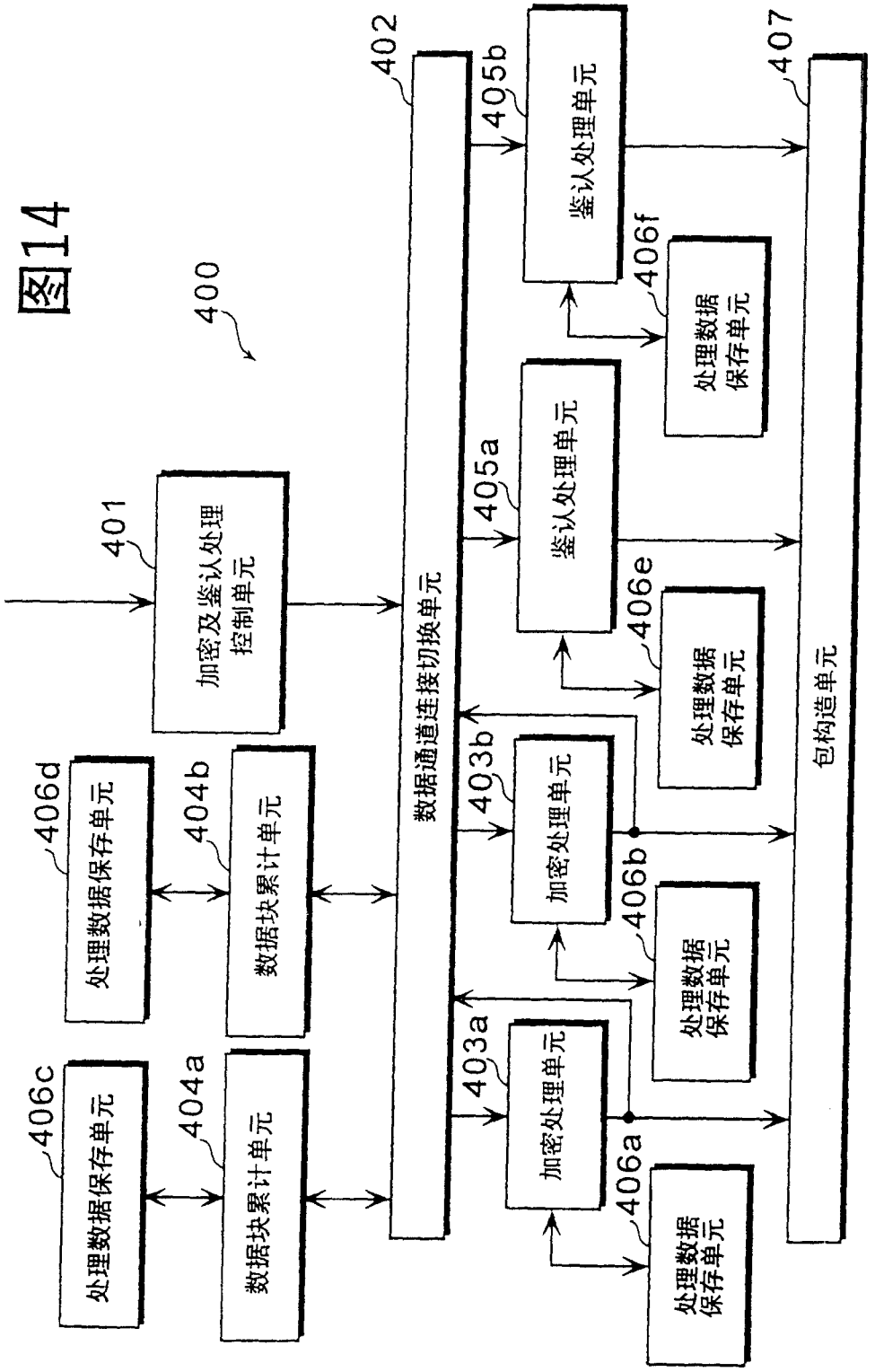

400
401
加密及鉴认处理控制单元
402
数据通道连接切换单元
403a
加密处理单元
403b
加密处理单元
404a
数据块累计单元
404b
数据块累计单元
405a
鉴认处理单元
405b
鉴认处理单元
406a
处理数据保存单元
406b
处理数据保存单元
406c
处理数据保存单元
406d
处理数据保存单元
406e
处理数据保存单元
406f
处理数据保存单元
407
包构造单元

图15

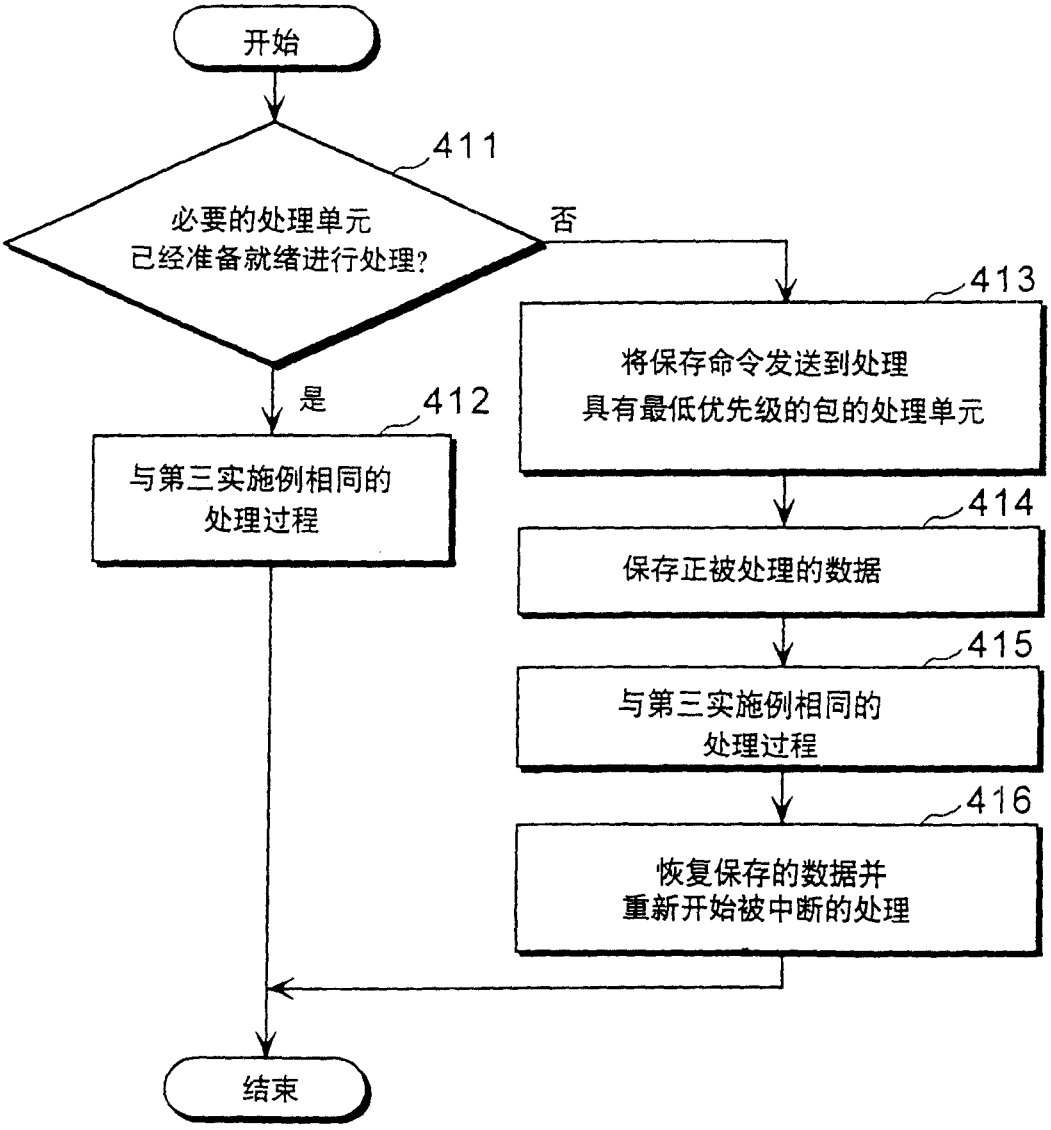

开始
411
必要的处理单元
已经准备就绪进行处理?
否
是
412
与第三实施例相同的
处理过程
413
将保存命令发送到处理
具有最低优先级的包的处理单元
414
保存正被处理的数据
415
与第三实施例相同的
处理过程
416
恢复保存的数据并
重新开始被中断的处理
结束

图16

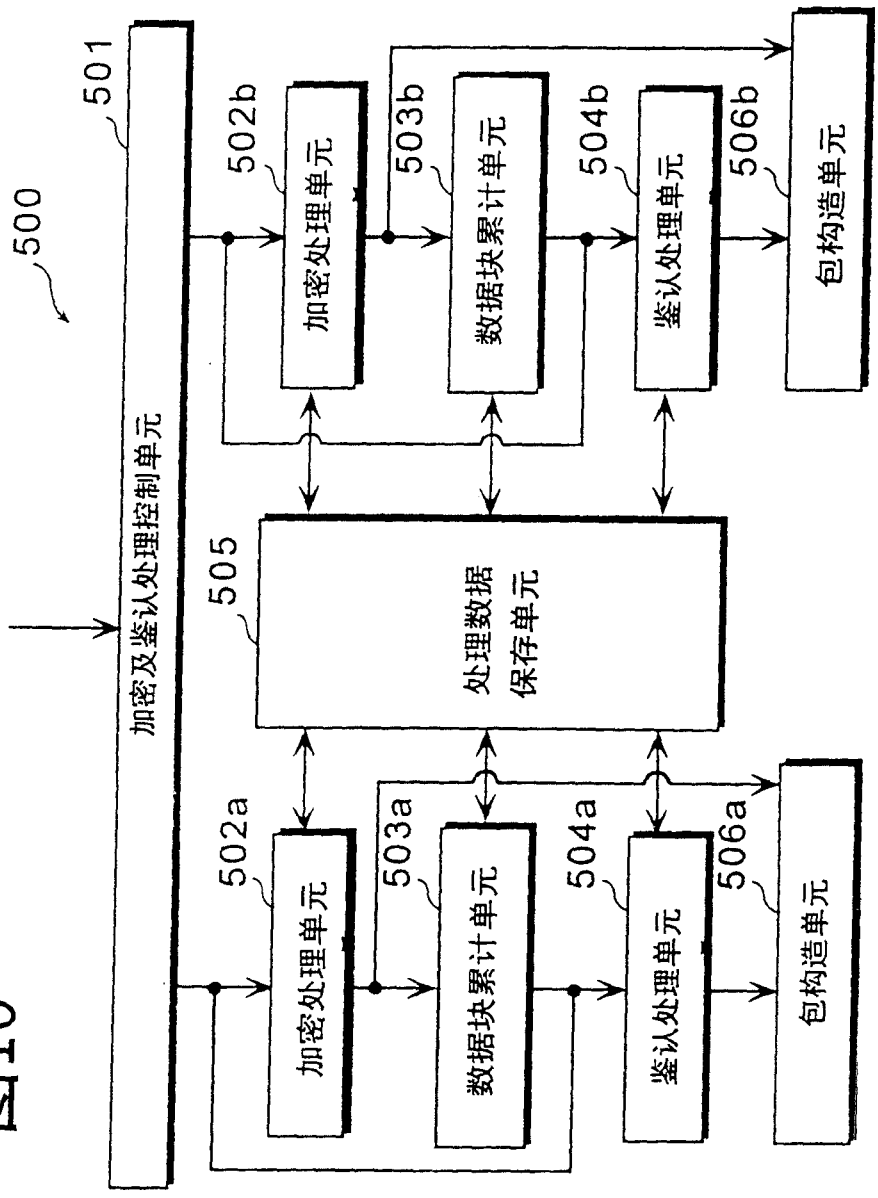

500
501
加密及鉴认处理控制单元
502b
加密处理单元
503b
数据块累计单元
504b
鉴认处理单元
506b
包构造单元
505
处理数据
保存单元
502a
加密处理单元
503a
数据块累计单元
504a
鉴认处理单元
506a
包构造单元

图17

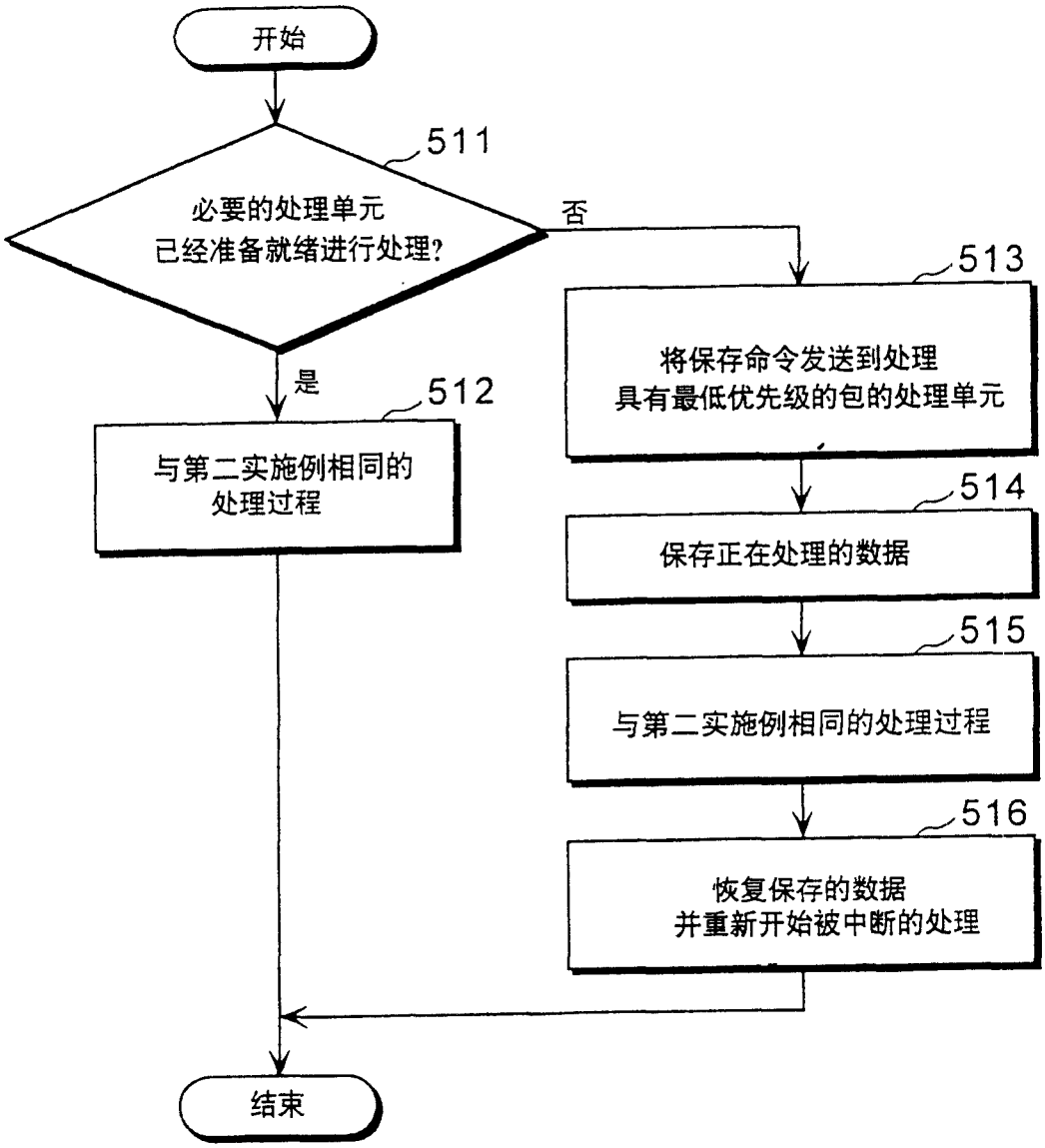
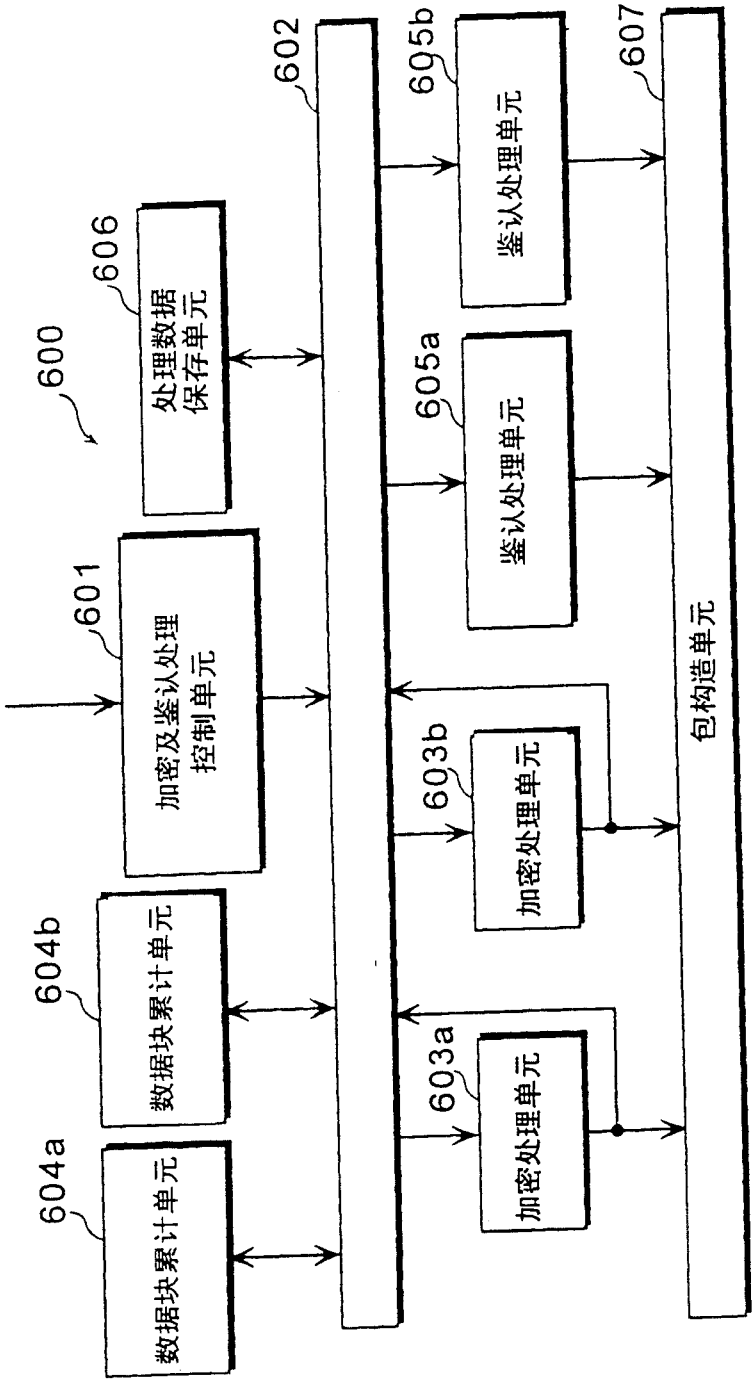

开始
511
必要的处理单元
已经准备就绪进行处理?
否
是
512
与第二实施例相同的
处理过程
513
将保存命令发送到处理
具有最低优先级的包的处理单元
514
保存正在处理的数据
515
与第二实施例相同的处理过程
516
恢复保存的数据
并重新开始被中断的处理
结束

图18


600
601
加密及鉴认处理控制单元
602
603a
加密处理单元
603b
加密处理单元
604a
数据块累计单元
604b
数据块累计单元
605a
鉴认处理单元
605b
鉴认处理单元
606
处理数据保存单元
607
包构造单元