



[12] 发 明 专 利 说 明 书

[21] ZL 专利号 98115064.0

[45] 授权公告日 2004 年 7 月 7 日

[11] 授权公告号 CN 1157020C

[22] 申请日 1998.4.22 [21] 申请号 98115064.0
[30] 优先权
[32] 1997. 4. 23 [33] JP [31] 105609/1997
[71] 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 大森基司 松崎夏目 馆林诚
丸山征克
审查员 李 卉

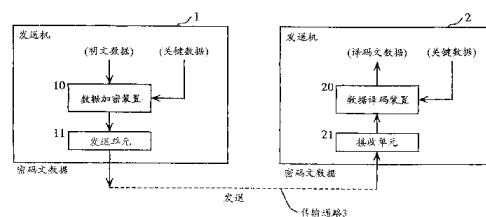
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 叶恺东 王忠忠

权利要求书 2 页 说明书 67 页 附图 50 页

[54] 发明名称 提高了安全性的密码处理装置

[57] 摘要

根据输入数据进行密码处理生成输出数据的密码处理装置, 包含有: 存贮用于为使前面密码处理影响后面的密码处理的链结数据、每次执行密码处理均更新该链结数据的存贮装置, 将存贮装置存贮的链结数据组合(融合)进输入数据生成组合数据的组合装置, 和根据组合数据执行主密码处理生成输出数据而在直至生成输出数据为止的过程中输出所生成的中间数据的主密码处理装置。其中, 存贮装置将主密码处理装置输出的中间数据作为新链结数据更新自身存贮的链结数据供下次密码处理之用。



1、密码处理装置，根据输入数据进行密码处理生成输出数据，其特征是包含：

5 一存贮装置，存贮为使前面密码处理影响后面的密码处理用的链结数据，每次进行密码处理时更新该链结数据；

一变换装置，对所述存贮装置存贮的链结数据进行预先确定的位置换或位变换生成变换数据；

一组合装置，将变换数据组合到输入数据生成组合数据；

10 一主密码处理装置，(a)根据组合数据执行主密码处理生成输出数据，(b)在直至生成输出数据的过程中输出所生成的中间数据，

其中，存贮装置将中间数据、输入数据、变换数据或输出数据作为新链结数据更新自身存贮的链结数据，供下次密码处理用。

2、权利要求1所述的密码处理装置，其特征是：

15 所述输入数据包含关键数据和被作密码处理数据；

所述组合装置将所述变换数据组合进关键数据生成组合关键数据；

所述主密码处理装置执行由组合链数据指定的主密码处理，由被作密码处理数据生成输出数据；

20 所述存贮装置将中间数据、被作密码处理数据或输出数据作为新链结数据更新自身存贮的链结数据供下次密码处理用。

3、权利要求2所述的密码处理装置，其特征是还包含：

信息组准备装置，将所述被作密码处理数据分割成具有规定位数的信息组单位，逐个顺序准备下一应作处理的1信息组的被作密码处理数据，所述密码处理装置以信息组为单位进行密码处理；

25 尾数数据处理装置，由信息组准备装置将被作密码处理数据分割成信息组单位时所产生的不满信息组单位的尾数数据，生成与该尾数数据相同长度的输出数据。

4、权利要求3所述的密码处理装置，其特征是

所述尾数数据处理装置包含：

30 一数据匹配装置，由所述链结数据生成与所述尾数数据同长的尾数链结数

据;

一尾数数据组合装置, 将尾数链结数据组合到尾数数据, 生成与该尾数数据同长的输出数据。

- 5 5、权利要求3所述的密码处理装置, 其特征是
所述尾数数据处理装置包含:

一数据匹配装置, 由所述变换数据生成与所述尾数数据同长的匹配数据;

一尾数数据组合装置, 将匹配数据组合到尾数数据, 生成与该尾数数据同长的输出数据。

- 10 6、权利要求2所述的密码处理装置, 其特征是还包含:
一关键数据存贮装置, 存贮关键数据, 每次执行密码处理更新该关键数据, 其中, 所述组合装置将所述变换数据组合到关键数据存贮装置存贮的关键数据;

其中, 关键数据存贮装置存贮关键数据的初始值, 在处理最初的数据时应用, 将组合关键数据作为新的关键数据更新自身存贮的关键数据。

- 15 7、权利要求1所述的密码处理装置, 其特征是:

所述输入数据包含关键数据和被作密码处理数据;

所述组合装置将所述变换数据组合进被作密码处理数据, 生成组合被作密码处理数据;

- 20 所述主密码处理装置执行由关键数据指定的主密码处理, 由组合被作密码处理数据生成输出数据;

所述存贮装置将中间数据、被作密码处理数据、组合被作密码处理数据或输出数据作为新链结数据, 更新自身存贮的链结数据, 供下次密码处理用。

提高了安全性的密码处理装置

5 技术领域

本发明是根据密钥以信息组为单位对作密码处理数据进行加密或译码处理的密码处理装置、密码处理方法、和存贮密码处理程序的存贮媒体,特别是关于不致大幅度增大装置规模和处理时间等地提高安全性的技术。

10 背景技术

近年来,随着借助数字通信的汇款以及所有信息的通信的普及,对于保护作通信的重要信息不受第三者的窃听和篡改、提高安全性的技术的要求日益增高。为提高完全性的有效的技术之一是密码。

在采用密码的通信系统中,原始报文称为明文,将其涵意内容变换成
15 第三者难以理解的形式称为密码文。而这种变换称为加密,相反,将密码文复原成原始明文的逆变换称为译码。

加密和解密的变换内容由算法和作为其参数的密钥确定。算法指定由多种变换构成的变换族,密钥指定该族内的一个变换。通常,与装置的固定部分相对应的为算法,而密钥则在一个装置中时常被更换。

20 密码文以被窃听作为前提。以窃听者不具备的算法和密钥的信息来译码成为明文被叫做密码解码。

要进行密码解码的人员(下面称为“密码解码者”)在已知道密码文的前提下进行密码解码。

基本上仅由密码文确定秘密的明文和密钥的解码法称为“密码文单独
25 攻击”。而由数个不定的密码文与明文对确定秘密的密钥来确定对应于任意的密码文的明文的解码法称做“已知明文攻击”。

作为密码的一例,如伪随机数加法型密码。

这种密码是发送方与接收方秘密共有同一密钥,各自利用具有相同算

法的随机数发生器以此密钥作为种源产生规定位数(下称“信息组”)的随机数,在发送侧作的加密中由以信息组为单元对此随机数和明文进行各个对应位的“异或”运算来生成密码文;而在接收侧进行的译码中,由此信息组为单位对此随机数和密码文进行各对应位的“异或”运算来生成明文。

这里如设定明文的信息组单位为“M”、密码文的信息组单位为“C”、此随机数为“R”、各对应位的“异或”运算为“(+)”,则加密和译码可分别表示成如下的(式1)和(式2):

$$C=M(+)R \quad (\text{式 1})$$

$$M=C(+)R \quad (\text{式 2})$$

这种密码的问题在于“已知明文处理”非常软弱。

例如,如果已知各自一信息组的明文和密码文时,按下(式3)就能由随机数R的判定来解码其他所有的明文:

$$R=M(+)C \quad (\text{式 3})$$

因而,密码解码者利用已知明文处理就能很容易地解码伪随机数加法型密码。

借助已知明文处理也较不容易解码的示例有DES(Data Encryption Standard, 数据加密标准)和FEAL(Fast Data Encipherment Algorithm,快速数据加密算法)。对此,在“密码理论入门”(冈本荣司著,共立出版社)中有详细说明。

这些密码以64位作为1信息组,以信息组为单位强力地搅乱数据。例如,DES的算法重复16层次进行转置和置换的组合处理。

为增强对密码解密和主动的非法动作的DES,开发了密码文信息组链的方式(Cipher Block Chaining)(以下称作“CBC方式”)。CBC方式在“近代密码理论”(池野信一、小山谦二著:电子情报通信学会发行)P66~67中有详细说明。

图1表示实现CBC方式的加密装置30的结构。

加密装置30由“异或”单元301、数据加密单元302、和寄存器303

构成。

寄存器 303 保存紧前面作加密处理的 1 信息组的密码文。在对起头的信息组进行加密时设定 1 信息组的初始值 IV (Initial Value)。

“异或”单元 301 对寄存器 303 保存的紧前面的 1 信息组的密码文和
5 下面应作加密的（信息组的明文进行每一对应位的“异或”运算，送往数据加密单元 302。而在对起始信息组进行加密时对初始值 IV 和起始的 1 信息组的明文进行每一对应位的“异或”运算。

数据加密单元 302 根据 64 位的关键数据以 DES 的算法时由“异或”单元 301 送来的 64 位的数据进行加密处理。

10 此加密装置 30 以信息组为单位对初始值 IV 和起始 1 信息组明文进行每一对应位的“异或”运算。根据 64 位关键数据进行加密生成 1 信息组密码文，再对此密码文和下一信息组的明文进行每一对应位的“异或”运算作为下一加密的输入。

如以信息组单位的明文作为 M_i ，信息组单位的密码文为 C_i (i 为信息
15 组序号， $i=2,3,\dots$)，以 64 位的关键数据作为 K ，应用关键数据 K 的加密作为 E_K ，以每一对应位的“异或”运算作为“ $(+)$ ”，则 CBC 方式可以下式(式 4)、(式 5)表示：

$$C_1 = E_K(M_1(+))IV \quad (\text{式 4})$$

$$C_i = E_K(M_i(+))C_{i-1} \quad (\text{式 5})$$

$$(i=2,3,\dots)$$

20 在 CBC 方式中，由于各 C_i 依赖于 C_i 之前的所有的密码文数据，所以就打乱了明文的统计性的特点。

因此就加强了对密码解码和主动非法动作的对策。

上述的 DES、FEAL 和 DES 中的 CBC 方式等的问题所在是，由于算
25 法成为公开时密钥的长度是有限制的，所以在“已知明文攻击”中，依靠逐个地利用全部密钥来试着进行加密，终究必然会发现正确的密钥。而 DES 的密钥长度虽如前述能为 64 位而因为有奇偶校验位的 8 位所以有效长为 56 位，可能取的密钥的数量是 2×56 个。

对 DES 这样的 56 位的密钥长，认为以花费庞大成本的现代技术水平

不断的试探就有可能解码。然而，如果采用多个独立的密钥作多重加密，按现在的技术水平就不再可能依靠不断的试探来解码。

但是，鉴于计算机的处理能力这十数年来已得到极其急剧的提高，不管如何作多重加密也不能断言今后有可能由不断的试探来解码的时日不会到来。

虽然越作多重加密安全性也提高，但如单独地为作多重加密来改变现有的装置，由于装置规模和处理时间等大幅度增加而是极不希望的。

为提高非多重加密的 CBC 模式等的安全性的历来技术在日本专利申请特开昭 52-130504 号公报（密码处理装置）、特公平 8-12537 号公报（加密装置）中有说明。前者根据密码文字的密码处理结果更新下一密码处理中用的关键数据。后者预先由密码密钥生成多个中间密钥加以存贮，根据依靠分别进行应用各中间密钥的位变换生成的各中间密钥更新信息，分别更新各中间密钥。

但是在上述历来的密码处理装置中不能断言充分确保安全性，而希望进一步提高安全性。

发明内容

因此，本发明就是针对这样的问题，目的就是要提供不致大幅度增大装置规模和处理时间等而能提高安全性的密码处理装置、密码处理方法、和存贮密码处理程序的存贮媒体。

为达到上述目的，根据本发明的密码处理装置，根据输入数据进行密码处理生成输出数据，其特征是包含：一存贮装置，存贮为使前面密码处理影响后面的密码处理用的链结数据，每次进行密码处理时更新该链结数据；一变换装置，对所述存贮装置存贮的链结数据进行预先确定的位置换或位变换变换生成变换数据；一组合装置，将变换数据组合到输入数据生成组合数据；一主密码处理装置，

25 (a) 根据组合数据执行主密码处理生成输出数据，(b) 在直至生成输出数据的过程中输出所生成的中间数据，其中，存贮装置将中间数据、输入数据、变换数据或输出数据作为新链结数据更新自身存贮的链结数据，供下次密码处理用。

按照这种构成，将执行密码处理的过程中所生成的中间数据作为链接数据存贮，在后面的密码处理时合并到关键数据或被作密码处理的数据等

的输入数据中，在每次执行密码处理时更新该链结数据，因此各输出数据即依赖于其本身之前的全部数据，明文的统计特征被各链结数据搅乱，所以尽管使密码解码很困难而并不那么增大装置规模和处理时间等。而密码解码者即使能得到密码文和明文对，事实上也不可能获得密码处理中所应用的链结数据，而且由于生成链结数据的算法和链结数据的初始值是不公开的，利用“已知明文攻击”进行破译密码更困难，也难以由不断的试探来解码。

因此能不大幅度增加装置规模和处理时间等使得安全性提高。

由以下结合说明本发明一特定实施例的附图所作叙述将会清楚了解本发

10 本发明的这些以及其他的目的、优点和特征。

附图说明：

- 图 1 表示实现 CBC 方式的加密装置 30 的结构；
- 图 2 表示本发明实施例 1 中密码通信系统的结构；
- 图 3 表示本发明实施例 1 中数据加密装置 10 的详细结构；
- 15 图 4 表示第 1~8 加密单元 105a~105h 的详细结构；
- 图 5 表示计算函数“f”部分的详细结构；
- 图 6 表示选择函数 S1~S8 的换字表；
- 图 7 表示本发明实施例 1 中尾数数据处理单元 106 的详细结构；
- 图 8 表示本发明实施例 1 中的数据译码装置 20 的详细结构；
- 20 图 9 表示本发明实施例 1 中尾数数据处理单元 206 的详细结构；
- 图 10 表示本发明实施例 1 的数据加密装置 10 中的加密处理的流程；
- 图 11 表示本发明实施例 1 的数据译码装置 20 中加密处理的流程；
- 图 12 表示本发明实施例 2 中数据加密装置 10 的详细结构；
- 25 图 13 表示本发明实施例 2 中数据译码装置 20 的详细结构；
- 图 14 表示本发明实施例 2 的数据加密装置 10 中加密处理流程；
- 图 15 表示本发明实施例 2 的数据译码装置 20 中加密处理的流程；
- 图 16 表示本发明实施例 3 中数据加密装置 10 的详细结构；

图 17 表示本发明实施例 3 中数据译码装置 20 的详细结构;

图 18 表示本发明实施例 3 的数据密码装置 10 中的加密处理流程;

图 19 表示本发明实施例 3 的数据译码装置 20 中加密处理流程;

5 图 20 表示本发明实施例 4 中数据加密装置 10 的详细结构;

图 21 表示本发明实施例 4 中数据译码装置 20 的详细结构;

图 22 表示本发明实施例 4 的数据加密装置 10 中加密处理流程;

图 23 表示本发明实施例 4 的数据译码装置 20 中加密处理流程;

图 24 表示本发明实施例 5 中数据加密装置 10 的详细结构;

10 图 25 表示本发明实施例 5 中数据译码装置 20 的详细结构;

图 26 表示本发明实施例 5 中数据加密装置 10 中加密处理流程;

图 27 表示本发明实施例 5 数据译码装置 20 中的加密处理流程;

图 28 表示本发明实施例 6 中数据加密装置 10 的详细结构;

图 29 表示本发明实施例 6 中数据译码装置 20 的详细结构;

15 图 30 表示本发明实施例 6 数据加密装置 10 中加密处理流程;

图 31 表示本发明实施例 6 数据译码装置 20 中的加密处理流程;

图 32 表示本发明实施例 7 中数据加密装置 10 的详细结构;

图 33 表示本发明实施例 7 中数据译码装置 20 的详细结构;

图 34 表示本发明实施例 7 数据加密装置 10 中的加密处理流程;

20 图 35 表示本发明实施例 7 数据译码装置 20 中的加密处理流程;

图 36 表示本发明实施例 8 中数据加密装置 10 的详细结构;

图 37 表示本发明实施例 8 中数据译码装置 20 的详细结构;

图 38 表示本发明实施例 8 的数据加密装置 10 中的加密处理流程;

25 图 39 表示本发明实施例 9 中数据加密装置 10 的详细结构;

图 40 表示本发明实施例 9 中数据译码装置 20 的详细结构;

图 41 表示本发明实施例 10 中数据加密装置 10 的详细结构;

图 42 表示本发明实施例 10 中数据译码装置 20 的详细结构;

图 43 表示本发明实施例 10 的数据密码装置 10 中加密处理流

程；

图 44 表示本发明实施例 10 的数据译码装置 20 中加密处理流程；

图 45 表示本发明实施例 11 中数据加密装置 10 的详细结构；

图 46 表示本发明实施例 11 中数据译码装置 20 的详细结构；

5 图 47 表示本发明实施例 11 的数据加密装置 10 中的加密处理流程；

图 48 表示本发明实施例 11 的数据译码装置 20 中的加密处理流程；

图 49 表示本发明实施例 12 中尾数数据处理单元 106 的详细结构；

10 图 50 表示本发明实施例 12 的数据加密装置 10 中的尾数数据处理流程。

具体实施方式

实施例 1

本发明的实施例 1 执行由关键数据指定的加密处理或译码处理（加密
15 处理或译码处理同时被称之为“密码处理”），为由明文数据生成密码文数据的加密装置和由密码文数据生成明文数据的译码装置（加密装置或译码装置共同被称为“由被作密码处理数据生成输出数据的密码处理装置”），在每次以信息组为单位执行密码处理时将在直至生成 1 信息组的输出数据为止所执行密码处理的过程中所生成的中间信息组作为链结信息
20 息组存贮，并在执行下一信息组的密码处理时将所存贮的链结信息组合并到关键数据的密码处理装置。

图 2 表示本发明实施例 1 中的密码通信系统的结构。

此密码通信系统由将明文数据加以加密发送的发送机 1 和接收密码文加以译码的接收机 2 组成。在同一图上还表明由发送机 1 向接收机 2
25 传送密码文数据的传输通路 3。

发送机 1 如图 2 中所示备有数据加密装置 10 和发送单元 11。

数据加密装置 10 取得明文数据，根据预设的关键数据将每一由规定的位数构成的信息组按规定算法进行加密，由得到的明文数据来生成密码文数据。这里所用的关键数据是发送机 1 和接收机 2 预先秘密地共有的，

规定的算法是装置固有的，指定变换族，而由此关键数据指定该族中的一个变换。而明文数据为将声音、图象信息和字符代码等进行数字编码后的数字信息。在此将由规定位数构成的1信息组例如作为64位来加以说明。

- 5 发送单元11将密码文数据作调制、放大等之后的发送数据送到传输通路3。

接收机2如图2中所示，备有数据译码装置20和接收单元21。

接收单元21通过传输通路3接收发送数据，将作解调等之后的密码文数据送到数据译码装置20。

- 10 数据译码装置20根据关键数据将各信息组按规定的算法进行译码，由密码文数据生成明文数据。

图3表示本发明实施例1中的图2所示数据加密装置10的详细结构。

- 此数据加密装置10由信息组分割单元101、信息组存贮单元102、关键数据合并单元103、部分密钥生成单元104、第1~8加密单元105a~105h、尾数数据处理单元106和信息组结合单元107构成。

- 图1中所示历来的编码化装置30和图3中所示本发明的实施例1中的数据加密装置10的关系是：“异或”单元301与关键数据组合单元103相对应，数据加密单元302与信息组分割单元101、部分密钥生成单元104、第1~8加密单元105a~105h、尾数数据处理单元106和信息组结合单元107相对应，寄存器303与信息组存贮单元102相对应。

- 信息分割单元101将获得的明文数据分割成64位组成的明文数据的1信息组（下称“明文信息组”）单位，顺次向第1加密单元105a传送，最后在生成不满64位的尾数明文数据时，将该尾数明文数据传送给尾数数据处理单元106。这里，例如得到200位的明文数据，从头开始分割成1~64bit的第一信息组、65~128bit的第二明文信息组、129~192bit的第三明文信息组和193~200bit的尾数明文数据，顺次将第一~三明文信息组向第1加密单元105a、将尾数明文数据向尾数数据处理单元106传送。

信息组存贮单元102在处理信息组分割单元101分割的各信息组时，

存贮为使前面的信息组影响到后面的信息组用的链结信息组。而在处理最初的信息组时，预先存贮链结信息组的初始值 IV。

关键数据组合单元 103 将信息组存贮单元 102 中所存贮的链结信息组合并到关键数据生成组合关键数据。在此，取得预先设定的 64 位的关键数据，在处理第一明文信息组时，对 64 位的链结信息组的初始值 IV 和 64 位的关键数据进行各对应的位的“异或”运算，在处理第二、三明文信息组时，对第一、二明文信息组处理时所生成的 64 位的链结信息组与 64 位的关键数据进行各对应的位的“异或”运算。

部分密钥生成单元 104 由关键数据组合单元 103 生成的组合关键数据生成相当于加密单元数量的数的部分密钥。在此，由 64 位的组合关键数据生成 8 个 48 位的部分密钥。

第 1 加密单元 105a 根据第一部分密钥由明文信息组生成第一中间信息组。

第 2~7 加密单元 105b~105g 各自根据第 2~7 的部分密钥由第 1~6 中间信息组生成第 2~7 中间信息组。

第 8 加密单元 105h 根据第 8 部分密钥由第 7 中间信息组生成密码文数据的 1 信息组（下称“密码文信息组”）。

第 1~8 加密单元 105a~105h 全都具有同样的结构，按照由 48 位的部分密钥所指定的变换，应用 64 位的输入内的低位 32 位变换高位 32 位，各自串行地进行调换高位 32 位与低位 32 位的变换，合计进行 8 级的此变换。在此，由第 1~3 明文信息组生成各个对应的第 1~7 中间信息组和第 1~3 密码文信息组。

图 4 表示第 1~8 加密单元 105a~105h 的详细结构。

64 位的明文信息组被分割成高位 32 位和低位 32 位，如将它们的高位作为 H_0 、低位作为 L_0 、第 n 加密单元的输入作为 $(H(n-1), L(n-1))$ 、输出作为 (H_n, L_n) ，则 H_n 、 L_n 以下面的（式 6）、（式 7）表示：

$$H_n = L(n-1) \quad (\text{式 6})$$

$$L_n = H(n-1) (+) f(L(n-1), K_n) \quad (\text{式 7})$$

这里，“(+)”是指各对应的位的“异或”运算，“ K_n ”为被输入

到第 n 加密单元的 48 位的部分密钥，“ f ”为采用 $L(n-1)$ 与 K_n 输出 32 位的数据的函数。

图 5 表示计算函数“ f ”的部分的详细结构。

32 位的 $L(n-1)$ 按以下（表 1）所示的扩展转置 E 被扩展并转变为 5 48 位。

（表 1）

	32	1	2	3	4	5
	4	5	6	7	8	9
10	8	9	10	11	12	13
	12	13	14	15	16	17
	16	17	18	19	20	21
	20	21	22	23	24	25
	24	25	26	27	28	29
15	28	29	30	31	32	1

表中的数值表示输入位置换的新的位的位置，例如，输入的第 32 位被置换为输出的第 1 位和第 47 位，输入的第 1 位被置换为输出的第 2 位和第 48 位。

20 对此 48 位和 48 位的部分密钥 K_n 进行各对应的位的“异或”EXOR 运算，再将该结果分割成各 6 位的 8 组，分别输入给 8 个选择函数 $S1 \sim S8$ 。

选择函数 $S1 \sim S8$ （也称为 S 逻辑单元）为输入 6 位输出 4 位的函数，其处理内容以换字表表示。

25 图 6 表示选择函数 $S1 \sim S8$ 的换字表。

在一个选择函数中，0 至 15 的数字为 64 个，排列成 4 行 16 列。

所输入的 6 位中的起始和最后位指定此换字表的行，除起始和最后外的 4 位指定列。

例如，在选择函数 $S1$ 中输入“011011”时由起始位“0”和最后位“1”

指定为第 2 行，由除起始和最后之外的 4 位“1101”指定为第 14 列。而由于选择函数 S1 的换字表的 2 行 14 列为“5”，故输出“0101”。

8 个选择函数 S1~S8 输出的合计 32 位（4 位×8=32 位）的输出成为进行下（表 2）中所示的转置 P 的“f(L(n-1)、Kn）”的输出。

5 （表 2）

		16	7	20	21
		29	12	28	17
		1	15	23	26
10		5	18	31	10
		2	8	24	14
		32	27	3	9
		19	13	30	6
		22	11	4	25
15					

表中的数值表示输入位置换的新的位的位置，例如，输入的第 16 位被置换成输出的第一位，输入的第 7 位被置换成输出的第二位。

信息组存贮单元 102 备有信息组更新功能，在每次第 4 加密单元 105d 生成第 4 中间信息组时，将此第 4 中间信息组作为新的链结信息组更新存贮的链结信息组，在下一信息组处理时应用。在此，预先存贮 64 位的初始值 IV，在处理第一明文信息组时应用此初始值 IV，将此处理时所生成的第 4 中间信息组更新为新的链结信息组。在处理第 2 明文信息组时应用第一明文信息组处理时更新的链结信息组，将此处理时所生成的第 4 中间信息组更新为新的链结信息组。接着在处理第 3 明文信息组时应用第 2 明文信息组处理时更新的链结信息组，将此处理时所生成的第 4 中间信息组更新为新的链结信息组。最后，在处理尾数明文数据时应用第 3 明文信息组的处理时更新的链结信息组。

尾数数据处理单元 106 由信息组分割单元 101 接收尾数明文数据，根据信息组存贮单元 102 中所存贮的链结信息组，由尾数明文数据生成与尾

数明文数据相同位数的尾数密码文数据,此处理单元 106 含有数据匹配单元 106a 和尾数数据组合单元 106b。

图 7 表示本发明实施例 1 中图 3 所示尾数数据处理单元 106 的详细结构。

- 5 数据匹配单元 106a 由信息组存贮单元 102 中存贮的链结信息组生成与尾数明文数据相同位数的尾数链结数据。在此,尾数明文数据为 8 位,生成由信息组存贮单元 102 中所存贮的链结信息组的例如高位 8 位构成的尾数链结数据。

- 尾数数据组合单元 106b 将尾数链结数据组合进尾数明文数据。这
10 里,对 8 位的尾数链结数据和 8 位的尾数明文数据进行各对应位的“异或”运算,生成 8 位的尾数密码文数据。

- 信息组结合单元 107 将第 8 加密单元 105h 生成的各密码文信息组与尾数数据处理单元 106 生成的尾数密码文数据相结合生成密码文数据。在此,将各 64 位的第 1~3 密码文信息组与 8 位的尾数密码文数据结合生成
15 200 位的密码文数据。

 信息组存贮单元 102 将链结信息组更新为第 4 加密单元 105d 生成的第 4 中间信息组,这仅为一例,由于以处理的过程生成的中间信息组怎样的均可,所以更新为第 1~7 加密单元 105a~105g 生成的第 1~7 中间信息组中的一个也可。

- 20 图 8 表示本发明实施例 1 中图 2 所示数据译码装置 20 的详细结构。

 此数据译码装置 20 由信息组分割单元 201、信息组存贮单元 202、关键数据组合单元 203、部分密钥生成单元 204、第 1~8 译码单元 205a~205h、尾数数据处理单元 206 和信息组结合单元 207 构成。

- 图 1 中所示加密装置 30 与图 8 中所示数据译码装置 20 的关系是:“异
25 或”单元 301 对应于关键数据组合单元 203,数据加密单元 302 对应于信息组分割单元 201、部分密钥生成单元 204、第 1~8 译码单元 205a~205h、尾数数据处理单元 206 和信息组结合单元 207,寄存器 303 对应于信息组存贮单元 202。

 信息组分割单元 201 将得到的密码文数据分割成 64 位组成的信息组

传送给第1译码单元205a,最后在生成不满64位的尾数密码文数据时,将该尾数密码文数据传送到尾数数据处理单元206。这里,作为一例,取得200位的密码文数据,由起头开始分割成为1~64位的第1密码文信息组,65~128位的第2密码文信息组,129~192位的第3密码文信息组和
5 193~200位的尾数密码文数据,将第1~3密码文信息组向第1译码单元205a传送,将尾数密码文数据向尾数数据处理单元206传送。

信息组存贮单元202在处理信息组分割单元201分割的各信息组时,存贮为要受到前面的信息组的影响而用的链结信息组。而在处理起始信息组时,预先存贮链结信息组的初始值IV。此初始值IV与数据加密装置10
10 中使用的值是同样的。某一明文数据的加密中用的初始值IV和与该明文数据对应的密码数据译码中用的初始值IV相同。

链结数据组合单元203将信息组存贮单元202中所存贮的链结数据组合进关键数据生成组合关键数据。此组合与数据加密装置10的关键数据组合单元10进行的组合相同。而此关键数据与数据加密装置10中使用的
15 相同。某明文数据的加密中间的关键数据和与该明文数据对应的加密数据的译码中用的关键数据相同。在此,预先取得所设定的64位关键数据,在处理第一密码文信息组时,对64位的链结信息组的初始值IV和64位的关键数据进行每一对应位的“异或”运算,在处理第2~3密码文信息组时,对第1~2密码文信息组的处理时所生成的64位的链结信息组和
20 64位的关键数据,进行每一对应位的“异或”运算。

部分密钥生成单元204由关键数据组合单元203生成的组合关键数据生成相当于译码单元数的数量的部分密钥。这里,由64位的组合关键数据生成8个48位的部分密钥。生成此部分密钥的功能与数据加密装置10的部分密钥生成单元104进行的那些全部相同。

25 第1译码单元205a根据第8部分密钥由密码文信息组生成第7中间信息组。

第2~7译码单元205b~205g各自根据第7~2的部分密钥由第7~2中间信息组生成第6~1中间信息组。

第8译码单元205h根据第1部分密钥由第1中间信息组生成明文信

息组。

第1~8译码单元205a~205h全都具有相同结构,按照由48位的部分密钥所指定的变换,利用64位的输入中的低位32位变换成高位32位,分别串行地进行高位32位与低位32位相交换的交换,合计进行8级此变换。这里,由第1~3密码文信息组生成其之各各对应的第7~1中间信息组和第1~3明文信息组。向第1~8译码单元205a~205h进行的变换分别为数据加密装置10的第8~1加密单元105h~105a的变换的逆变换。

信息组存贮单元202备有信息组更新功能,每次第4译码单元205d生成第4中间信息组时,将此第4中间信息组作为新的链结信息组来更新存贮着的链结信息组,在处理下一信息组时应用。在此,预先存贮有64位的初始值IV,此初始值IV在处理第一密码文信息组时被利用,将此处理时所生成的第4中间信息组作为新的链接数据存贮。接着,在第一密码文信息组处理时所更新的链结信息组被用于处理第二密码文信息组中,将此处理时所生成的第4中间信息组作为新链结信息组存贮。然后,第二密码文信息组处理时所存贮的链结数据在处理第3密码文信息组时加以利用,将此处理时所生成的第4中间信息组作为新链结信息组存贮。最后,在处理第3密码文信息组时存贮的链结信息组在处理尾数密码文数据时应用。

尾数数据处理单元206由信息组分割单元201接收尾数密码文数据,根据信息组存贮单元202中存贮的链结信息组,由尾数密码文数据生成与尾数密码文数据相同位数的尾数明文数据,此处理单元206含有数据匹配单元206a和尾数数据组合单元206b。

图9表示本发明实施例1中图8所示的尾数数据处理单元206的详细结构。

数据匹配单元206a由信息组存贮单元202中存贮的链结信息组生成与尾数密码文数据相同位数的尾数链结数据。在此,由于尾数密码文数据为8位,所以生成信息组存贮单元202中存贮的链结信息组的例如以高位8位构成的尾数链结数据。

尾数数据组合单元206b将尾数链结数据组合到尾数密码文数据。这

里,对8位的尾数链结数据和8位的尾数密码文数据进行每一对应位的“异或”运算,生成8位的尾数明文数据。

信息组结合单元207将第8译码单元205h生成的明文数据的各信息组和尾数数据处理单元206生成的尾数明文数据相结合生成明文数据。在此,将各64位的第1~3明文数据和8位的尾数明文数据相结合生成200位的明文数据。

信息组存贮单元202将链结信息组更新为第4译码单元205d生成的中间信息组,这只是这方面的一例,因为如果是处理过程中生成的中间信息组哪一个均可,所以也可以更新为第1~7译码单元205a~205g生成的第1~7中间信息组中的另一个。但是有必要更新为与数据加密装置10的信息组存贮单元102同一的中间信息组。

图10表示本发明实施例1的数据加密装置10中的加密处理流程。

这里作为一例,取得200位的明文数据,在信息组存贮单元102中作为被预先存贮的初始值IV,按DES的算法为基准进行说明。

(1)信息组分割单元101判断取得的明文数据的未处理部分有无64位以上(步骤S101)。在此,第一次因为取得的明文数据的未处理部分为200位所以判定为64位以上(步骤S101:第一次)。

(2)在明文数据的未处理部分为64位以上时,由未处理部分的起头分离64位(步骤S102)。在此,由200位中的起头起计数将1~64位分离为第1明文信息组(步骤S102:第一次)。

(3)关键数据组合单元103将信息组存贮单元102中存贮的链结信息块组合到关键数据,生成组合关键数据(步骤S103)。在此,对64位的链结信息组的初始值IV和64位的关键数据进行每一对应位的“异或”运算,生成组合关键数据传送到部分密钥生成单元104(步骤S103:第1次)。

(4)部分密钥生成单元104由组合关键数据生成相当于加密单元数的数量的部分密钥(步骤S104)。在此,由64位的组合关键数据生成8个48位的部分密钥(步骤S104:第1次)。

由含有 8 位的奇偶校验位的 64 位的关键数据生成第 1~8 个的 8 个×48 位的部分密钥的程序，例如，如下所述。

含有奇偶校验位的 64 位的关键数据通过（表 3）中所示的转置，成为在进行转置的同时除去奇偶位的 56 位。

5

（表 3）

10	57	49	41	33	25	17	9
	1	58	50	42	34	26	18
	10	2	59	51	43	35	27
	19	11	3	60	52	44	36
15	63	55	47	39	31	23	15
	7	62	54	47	38	30	22
	14	6	61	53	45	37	29
	21	13	5	28	20	12	4

表中的数值表示输入位置换的新的位的位置，例如，输入的第 57 位被置换为输出的第 1 位，输入的第 49 位被置换为输出的第 2 位。

20 在此 56 位中将前半 28 位作为 CO，后半 28 位作为 DO，将此 CO 和 DO 按（表 4）中所示的位移次数左移生成 C1~C8 和 D1~D8。

（表 4）

25	部分密钥号	1	2	3	4	5	6	7	8
	位移次数	2	4	8	12	16	20	24	26

例如，如 C0=（C1 C2 C3...C26 C27 C28），则成为 C1=（C3 C4 C5...C28 C1 C2）。

接着，将各个的 56 位按（表 5）所示的转置而成为 48 位。

(表 5)

	14	17	11	24	1	5
	3	28	15	6	21	10
5	23	19	12	4	26	8
	16	7	27	20	13	2
	41	52	31	37	47	55
	30	40	51	45	33	48
	44	49	39	56	34	53
10	46	42	50	36	29	32

表中的数值表示输入位置换的新的位的位置，例如，输入的第 14 位被置换成输出的第 1 位，输入的第 17 位被置换成输出的第 2 位。

(5) 第 1 加密单元 105a 根据第 1 的部分密钥由明文信息组生成第 1 中间信息组（步骤 S105）。在此，由第 1 明文信息组生成第 1 中间信息组（步骤 S105：第 1 次）。

(6) 第 2~4 加密单元 105b~105d 各自根据第 2~4 的部分密钥由第 1~3 中间信息组生成第 2~4 中间信息组（步骤 S106）。在此，由对应于第 1 明文信息组的第 1~3 中间信息组生成第 2~4 中间信息组（步骤 S106：第 1 次）。

(7) 信息组存贮单元 102 将第 4 中间信息组作为新的链结信息组，更新存贮中的链结信息组（步骤 S107）。在此，更新为对应于第 1 明文信息组的第 4 中间信息组（步骤 S107：第 1 次）。

(8) 第 5~7 加密单元 105e~105g 各自根据第 5~7 的部分密钥由第 4~6 中间信息组生成第 5~7 中间信息组（步骤 S108）。在此，由对应于第 1 明文信息组的第 4~6 中间信息组生成第 5~7 中间信息组（步骤 S108：第 1 次）。

(9) 第 8 加密单元 105h 根据第 8 的部分密钥由第 7 中间信息组生成密码文信息组（步骤 S109）。在此，由对应于第 1 明文信息组的第 7 中间信息组生成第 1 密码文信息组（步骤 S109：第 1 次）。

(10) 判断是否具有明文数据的未处理部分。在尚有未处理部分时，处理下一明文信息组或尾数明文数据，返回步骤 S101（步骤 S110）。这里尚存在未处理部分故返回步骤 S101（步骤 S110：第 1 次）。

(11) 在步骤 S101 中，这里第 1 次由 200 位的明文数据分离 64 位，
5 其剩余为 136 位，所以判定为 64 位以上（步骤 S101：第 2 次）。

(12) 在步骤 S102 中，这里由最初的 200 位的起头数起将第 65~128 位作为第 2 明文信息组加以分离（步骤 S102：第 2 次）。

(13) 在步骤 S103 中，这里对处理第 1 明文信息组时所生成的 64 位的链结信息组和 64 位的关键数据进行每一对应位的“异或”运算，生成组合关键数据传送到部分密钥生成单元 104（步骤 S103：第 2 次）。
10

(14) 在步骤 S104 中，这里由 64 位的组合关键数据生成 8 个 48 位的部分密钥（步骤 S104：第 2 次）。

(15)~(19) 在步骤 S105~步骤 S109 中对第 2 明文信息组进行与第 1 明文信息组同样的处理，生成对应于第 2 明文信息组的第 1~7 中间信息组和密码文信息组，将信息组存贮单元 102 中存贮的链接信息组更新为对应于第 2 明文信息组的第 4 中间信息组（步骤 S105~S109：第 2 次）。
15

(20) 在步骤 S110 中，这里由于尚有明文数据的未处理部分所以返回步骤 S101（步骤 S110：第 2 次）。

(21) 在步骤 S101 中，这里第 2 次由 136 位的明文数据分离 64 位，
20 因其剩余 72 位故判定为 64 位以上（步骤 S101：第 3 次）。

(22) 在步骤 S102 中，这里由最初的 200 位的起头数起将第 129~192 位作为第 3 明文信息组分离（步骤 S102：第 3 次）。

(23) 在步骤 S103 中，这里对处理第 2 明文信息组时所生成的链结信息组和 64 位的关键数据进行各对应位的“异或”运算，生成组合关键数据传送到部分密钥生成单元 104（步骤 S103：第 3 次）。
25

(24) 在步骤 S104 中，这里由 64 位的组合关键数据生成 8 个 48 位的部分密钥（步骤 S104：第 3 次）。

(25~29) 步骤 S105~S109 中，对第 3 明文信息组进行与第 1 明文信息组同样的处理，生成对应于第 3 明文信息组的第 1~7 中间信息组和密码文信息组，将信息组存贮单元 102 中存贮的链结信息组更新为对应于
30

第3明文信息组的第4中间信息组（步骤S105～S109：第3次）。

（30）步骤S110中，这里因尚有未处理的明文数据部分故返回步骤S101（步骤S110：第3次）。

（31）在步骤S101中，这里第3次72位的明文数据分离64位，因
5 剩余8位，判定为不满64位（步骤S101：第4次）。

（32）在明文数据的未处理部分不满64位时，将此未处理部分传送到尾数数据处理单元106（步骤S111）。这里由最初的200位的起头数起将第193～200位作为尾数明文数据传送到尾数数据处理单元106。

（33）尾数数据处理单元106由信息组分割单元101接收尾数明文数
10 据，根据信息组存贮单元102中存贮的链结信息组，由尾数明文数据生成与尾数明文数据相同位数的尾数密码文数据（步骤S112）。这里对处理信息组存贮单元102中存贮的第3明文信息组时所生成的64位链结信息组内的高8位和8位的尾数明文数据进行各对应位的“异或”运算，生成8位的尾数密码文数据。

（34）在步骤S110判断明文数据无未处理部分时，或者在步骤S112
15 中生成尾数密码文数据之后，信息组结合单元107将第8加密单元105h生成的各密码文信息组与尾数数据处理单元106生成的尾数密码文数据相结合生成密码文数据（步骤S113）。这里将与第1～3明文信息组各自对应的各密码文信息组与尾数密码文数据相结合生成200位的密码文数
20 据。

图11表示本发明实施例1的数据译码装置20中的加密处理流程。

数据译码装置20的操作为数据加密装置10的操作的逆变换。

这里作为一例，取200位的密码文数据，在信息组存贮单元202中与
数据加密装置10的信息组存贮单元102同样地预先存贮初始值IV，按照
25 DES的算法作为基准予以说明。

（1）信息分割单元201判断取得的密码文数据的未处理部分是否有64位以上（步骤S201）。这里第1次，因取得的密码文数据的未处理部分为200位故判定为64位以上（步骤S201：第1次）。

（2）在密码文数据的未处理部分为64位以上时自未处理部分的起头
30 开始分离64位（步骤S202）。这里由200位中的起头数起始第1～64位

作为第1密码文信息组分离（步骤 S202：第1次）。

（3）关键数据组合单元 203 将信息组存贮单元 202 中存贮的链结信息组组合进关键数据生成组合关键数据（步骤 S203）。这里对 64 位的链结信息组的初始值 IV 和 64 位的关键数据进行各对应位的“异或”运算，
5 生成组合关键数据传送到部分密钥生成单元 204（步骤 S203：第1次）。

（4）部分密钥生成单元 204 由组合关键数据生成相当于译码单元数的数量的部分密钥（步骤 S204）。这里由 64 位的组合关键数据生成 8 个 48 位的部分密钥（步骤 S204：第1次）。

由含有 8 位奇偶校验位的 64 位的关键数据生成第 1~8 的 8 个×48
10 位的部分密钥的程序与数据加密装置 10 的部分密钥生成单元 104 相同。

（5）第1译码单元 205a 根据第 8 个部分密钥由密码文信息组生成第 7 中间信息组（步骤 S205）。这里由第 1 密码文信息组生成第 7 中间信息组（步骤 S205：第1次）。

（6）第 2~4 译码单元 205b~205d 各自根据第 7~5 的部分密钥由第
15 7~5 中间信息组生成第 6~4 中间信息组（步骤 S206）。这里由对应于第 1 密码文信息组的第 7~5 中间信息组生成第 6~4 中间信息组（步骤 S206：第1次）。

（7）信息组存贮单元 202 将第 4 译码单元 205d 生成的第 4 中间信息组作为新的链结信息组更新存贮着的链结信息组（步骤 S207）。这里更
20 新为对应于第 1 密码文信息组的第 4 中间信息组（步骤 S207：第1次）。

（8）第 5~7 译码单元 205e~205g 各自根据第 4~2 的部分密钥由第 4~2 中间信息组生成第 3~1 中间信息组（步骤 S208）。这里由对应于第 1 密码文信息组的第 4~2 中间信息组生成第 3~1 中间信息组（步骤 S208：第1次）。

25 （9）第 8 译码单元 205h 根据第 1 的部分密钥由第 1 中间信息组生成明文信息组（步骤 S209）。这里由对应于第 1 密码文信息组的第 1 中间信息组生成明文信息组（步骤 S209：第1次）。

（10）判断是否存在密码文数据的未处理部分。在有未处理部分时处理下一密码文信息组或尾数密码文数据，返回步骤 S201（步骤 S210）。
30 这里尚存在未处理部分故返回步骤 S201（步骤 S210：第1次）。

(11) 在步骤 S201 中, 这里第 1 次由 200 位的密码文数据分离 64 位, 其剩余为 136 位, 所以判定为 64 位以上 (步骤 201: 第 2 次)。

(12) 在步骤 S202 中, 这里由最初的 200 位的起头数起将第 65~128 位作为第 2 密码文信息组分离 (步骤 S202: 第 2 次)。

5 (13) 在步骤 S203, 这里对处理第 1 密码文信息组时所生成的 64 位的链结信息组和 64 位的关键数据进行各对应位的“异或”运算, 生成组合关键数据传送到部分密钥生成单元 204 (步骤 S203: 第 2 次)。

(14) 在步骤 S204, 这里由 64 位的组合关键数据生成 8 个 48 位的部分密钥 (步骤 S204: 第 2 次)。

10 (15)~(19) 在步骤 S205~S209, 对第 2 密码文信息组进行与第 1 密码文信息组同样的处理, 生成对应于第 2 密码文信息组的第 7~1 中间信息组和明文信息组, 将信息组存贮单元 202 中存贮的链结数据更新为对应于第 2 密码文信息组的第 4 中间信息组 (步骤 S205~S209: 第 2 次)。

15 (20) 在步骤 S210, 这里因尚存在未处理的密码文数据部分而返回步骤 S201 (步骤 S210: 第 2 次)。

(21) 在步骤 S201 中, 这里第 2 次由 136 位的密码文数据分离 64 位, 因剩余 72 位而判定为 64 位以上 (步骤 S201: 第 3 次)。

(22) 在步骤 S202, 这里由最初的 200 位的起头数起将第 129~192 位作为第 3 密码文信息组分离 (步骤 S202: 第 3 次)。

20 (23) 在步骤 S203, 这里对处理第 2 密码文信息组时所生成的链结信息组和 64 位的关键数据进行各对应位的“异或”运算, 生成组合关键数据传送给部分密钥生成单元 204 (步骤 S203: 第 3 次)。

(24) 在步骤 S204, 这里由 64 位的组合关键数据生成 8 个 48 位的部分密钥 (步骤 S204: 第 3 次)。

25 (25)~(29) 在步骤 S205~S209, 对第 3 密码文信息组进行与第 1 密码文信息组相同的处理, 生成对应于第 3 密码文信息组的第 7~1 中间信息组和明文信息组, 将信息组存贮单元 202 存贮的链结数据更新为对应于第 3 密码文信息组的第 4 中间信息组 (步骤 S205~S209: 第 3 次)。

30 (30) 在步骤 S210, 这里因尚存在密码文数据的未处理部分故返回步骤 S201 (步骤 S210: 第 3 次)。

(31) 在步骤 S201 中, 这里第 3 次由 72 位的密码文数据分离 64 位, 其剩余为 8 位故制定为不足 64 位 (步骤 S201: 第 4 次)。

(32) 在密码文数据的未处理部分不足 64 位时, 将此未处理部分传送到尾数数据处理单元 206 (步骤 S211)。这里由最初的 200 位的起头数起将第 193~200 位作为尾数密码文数据传送到尾数数据处理单元 206。

(33) 尾数数据处理单元 206 由信息组分割单元 201 接收尾数密码文数据, 根据信息组存贮单元 202 中存贮的链结信息组, 由尾数密码文数据生成与尾数密码文数据相同位数的尾数明文数据 (步骤 S212)。这里对处理信息组存贮单元 202 中所存贮的第 3 密码文信息组时所生成的 64 位链结数据中的高 8 位和 8 位的尾数密码文数据进行各对应位的“异或”运算, 生成 8 位的尾数明文数据。

(34) 在步骤 S210 中判断无密码文数据的未处理部分时, 或在步骤 S212 中生成尾数明文数据后, 信息组结合单元 207 将各明文信息组与尾数数据处理单元 206 生成的尾数明文数据相结合生成明文数据 (步骤 S213)。这里将各自与第 1~3 密码文信息组对应的明文信息组与尾数明文数据结合生成 200 位的明文数据。

实施例 1 的密码处理装置是将在对前面的信息组执行密码处理过程中生成的中间信息组作为链结信息组存贮, 在后面的密码处理时组合到关键数据, 每次执行密码处理均要更新该链结信息组。

20 <实施例 2>

本发明实施例 2 与实施例 1 不同处在于, 不是将存贮的链结信息组组合到关键数而是组合到被作密码处理的数据或对被作密码处理数据执行密码处理后的数据。

密码通信系统的结构与实施例 1 相同, 其说明省略。

25 图 12 表示本发明实施例 2 中图 2 所示数据加密装置 10 的详细结构。

与实施例 1 中图 3 所示数据加密装置 10 共同的结构部分加以同一标号、具有同一功能的结构部分其说明省略。

此数据加密装置 10 由信息组分割单元 101、信息组存贮单元 102、部分密钥生成单元 104、第 1~8 加密单元 105a~105h、尾数数据处理单元 30 106, 信息组结合单元 107 和信息组组合单元 108 构成。

图1中所示历来的加密装置30与图12所示本发明实施例2中的数据加密装置10的关系是：“异或”单元301与信息组组合单元108对应，数据加密单元302与信息组分割单元101、部分密钥生成单元104、第1~8加密单元105a~105h、尾数数据处理单元106和信息组结合单元107相对应，寄存器303与信息组存贮单元102对应。

信息组分割单元101将分割的信息组不传送给第1加密单元105而传送给信息组组合单元108，仅这一点与实施例1不同。

信息组组合单元108将信息组存贮单元102中存贮的链结数据组合到明文信息组生成组合明文信息组。这里在处理第1明文信息组时对64位的链结信息组的初始值IV与64位的第1明文信息组进行各对应位的“异或”运算，生成64位的第1组合明文信息组，在处理第2~3明文信息组时，对第1~2明文信息组处理时所生成的64位的链结信息组与64位的第2~3明文信息组进行每一对应位的“异或”运算生成64位的第2~3组合明文信息组。

部分密钥生成单元104由关键数据生成相当于加密单元数的数量的部分密钥。这里获取预先所设定的64位的关键数据，由64位关键数据生成8个48位的部分密钥。

第1加密单元105a不由明文信息组而由信息组组合单元108生成的组合明文信息组生成第1中间信息组。

第1~8加密单元105a~105h具有与实施例1同一的功能。这里由第1~3组合明文信息组生成各自对应的第1~7中间信息组和第1~3密码文信息组。

图13表示本发明实施例2中的图2所示数据译码装置20的详细结构。

与实施例1图8所示数据译码装置20共同的结构部分加以同一标号，具有同一功能的构成部分的说明省略。

此数据译码装置20由信息组分割单元201、信息组存贮单元202、部分密钥生成单元204、第1~8译码单元205a~205h、尾数数据处理单元206、信息组结合单元207和信息组组合单元208构成。

部分密钥生成单元204由关键数据生成相当于译码单元数的数量的

部分密钥。这里获取预先设定的 64 位的关键数据，由 64 位的关键数据生成 8 个 48 位的部分密钥。此部分密钥的生成与数据加密装置 10 的部分密钥生成单元 104 进行的部分密钥的生成完全相同。

第 8 译码单元 205h 根据第 1 的部分密钥由第 1 中间信息组生成密码
5 处理信息组。

第 1~8 译码单元 205a~205h 具有与实施例 1 同样的功能。这里由第 1~3 密码文信息组生成各自对应的第 1~7 中间信息组和第 1~3 密码处理信息组。

信息组组合单元 208 将信息组存贮单元 202 中存贮的链结信息组组合
10 到密码处理信息组生成明文信息组。这里在处理第 1 密码文信息组 时，对 64 位的链结信息组的初始值 IV 与 64 位的第 1 密码处理信息组进行各对应位的“异或”运算，生成 64 位的第 1 明文信息组，在处理第 2~3 密码文信息组时对第 1~2 密码文信息组处理时所生成的 64 位链结信息组与 64 位的第 2~3 密码处理信息组进行每一对应位的“异或”运算，生成
15 64 位的第 2~3 明文信息组。

信息组结合单元 207 将信息组组合单元 208 生成的明文数据的各信息组与尾数数据处理单元 206 生成的尾数明文数据相结合生成明文数据。这里将各 64 位的第 1~3 明文数据与 8 位的尾数明文数据相结合生成 200 位的明文数据。

20 图 14 表示本发明实施例 2 的数据加密装置 10 中加密处理的流程。

与实施例 1 中图 10 所示数据加密装置 10 的操作共同的步骤加以同一标号，其说明省略。

(1) ~ (2) 与实施例 1 相同 (步骤 S101、S102: 第 1 次)。

(3) 部分密钥生成单元 104 由关键数据生成相当于加密单元数的数量的部分密钥 (步骤 S301)。这里获取予设定 64 位的关键数据，由 64
25 位关键数据生成 8 个 48 位的部分密钥 (步骤 S301: 第 1 次)。

(4) 信息组组合单元 108 将信息组存贮单元 102 中存贮的链结信息组组合进明文信息组生成组合明文信息组 (步骤 S302)。这里对 64 位的链结信息组的初始值 IV 与 64 位的第 1 明文信息组进行各对应位的“异
30 或”运算，生成 64 位的第 1 组合明文信息组 (步骤 S302: 第 1 次)。

(5)第1加密单元105a根据第1部分密钥由组合明文信息组生成第1中间信息组(步骤S303)。在此由第1组合明文信息组生成第1中间信息组(步骤S303:第1次)。

(6)~(12)与实施例1相同(步骤S106~S110:第1次,步骤5 S101、S102:第2次)。

(13)在步骤S301,这里由64位的关键数据生成8个48位的部分密钥。而如果关键数据不变化因与第1次完全相同,所以也可以存贮各部分密钥(步骤S301:第2次)。

(14)在步骤S302,这里对第1明文信息组处理时所生成的64位链10 结信息组与64位的第2明文信息组进行各对应位的“异或”运算,生成64位的第2组合明文信息组(步骤S302:第2次)。

(15)在步骤S303中,这里由第2组合明文信息组生成第1中间信息组(步骤S303:第2次)。

(16)~(22)与实施例1相同(步骤S106~S110:第2次,步骤15 S101、S102:第3次)。

(23)在步骤S301,这里由64位的关键数据生成8个48位的部分密钥。而如果关键数据不变更则与第1次完全相同的处理,所以可不管存贮的各部分密钥(步骤S301:第3次)。

(24)在步骤S302中,这里对第2明文信息组处理时所生成的6420 位的链结信息组与64位的第3明文信息组进行各对应位的“异或”运算,生成64位的第3组合明文信息组(步骤S302:第3次)。

(25)在步骤S303,这里由第3组合明文信息组生成第1中间信息组(步骤S303:第3次)。

(26)~(34)与实施例1相同(步骤S106~S110:第3次,步骤25 S101:第4次,步骤S111~S113)。

图15表示本发明实施例2的数据译码装置20中加密处理流程。

数据译码装置20的操作为数据加密装置10的操作的逆变换。

与实施例1中图11所示数据译码装置20的操作共同的步骤加以相同标号,其说明省略。

30 (1)~(2)与实施例1相同(步骤S201~S202:第1次)。

(3) 部分密钥生成单元 204 由关键数据生成相当于译码单元数的数量的部分密钥 (步骤 S401)。这里获取预先设定的 64 位的关键数据, 由此 64 位关键数据生成 8 个 48 位的部分密钥 (步骤 S401: 第 1 次)。

(4) ~ (6) 与实施例 1 的 (5)、(6)、(8) 相同 (步骤 S205、
5 S206、S208: 第 1 次)。

(7) 第 8 译码单元 205h 根据第 1 部分密钥由第 1 中间信息组生成密码处理信息组 (步骤 S402)。这里由对应于第 1 密码文信息组的第 1 中间信息组生成第 1 密码处理信息组 (步骤 S402: 第 1 次)。

(8) 信息组组合单元 208 将信息组存贮单元 202 中存贮的链结数据
10 组合进密码处理信息组生成明文信息组 (步骤 S403)。在此时 64 位的链结信息组的初始值 IV 与 64 位的第 1 密码处理信息组进行各对应位的“异或”运算, 生成 64 位的第 1 明文信息组 (步骤 S403: 第 1 次)。

(9) 与实施例 1 的 (7) 相同 (步骤 S207: 第 1 次)。

(10) ~ (12) 与实施例 1 相同 (步骤 S210: 第 1 次, 步骤 S201 ~
15 S202: 第 2 次)。

(13) 在步骤 S401, 这里由 64 位的关键数据生成 8 个 48 位的部分密钥。而如果关键数据不变更因与第 1 次为完全同样的处理, 可以不管所存贮的各部密钥如何 (步骤 S401: 第 2 次)。

(14) ~ (16) 与实施 1 的 (15)、(16)、(18) 相同 (步骤 S205、
20 S206、S208: 第 2 次)。

(17) 在步骤 S402, 这里由对应于第 2 密码文信息组的第 1 中间信息组生成第 2 密码处理信息组 (步骤 S402: 第 2 次)。

(18) 在步骤 S403, 这里对在第 1 密码文信息组处理时生成的 64 位的链结数据与 64 位的第 2 密码处理信息组进行每一对应位的“异或”运算生成 64 位的第 2 明文信息组 (步骤 S403: 第 2 次)。
25

(19) 与实施例 1 的 (17) 同样 (步骤 S207: 第 2 次)。

(20) ~ (22) 与实施例 1 相同 (步骤 S210: 第 2 次, 步骤 S201 ~
S202: 第 3 次)。

(23) 步骤 S401 中, 这里由 64 位的关键数据生成 8 个 48 位的部分
30 密钥。而如关键数据不变更则因与第 1 次为完全相同的处理, 所以可不管

所存贮的各部分密钥如何（步骤 S401：第 3 次）。

（24）～（26）与实施例 1 的（25）、（26）、（28）相同（步骤 S205、S206、S208：第 3 次）。

（27）在步骤 S402，这里由对应于第 3 密码文信息组的第 1 中间信息组生成第 3 密码处理信息组（步骤 S402：第 3 次）。

（28）步骤 S403 中，这里对第 2 密码文信息组处理时生成的 64 位的链结信息组与 64 位的第 3 密码处理信息组进行每一对应位的“异或”运算生成 64 位的第 3 明文信息组（步骤 S403：第 3 次）。

（29）与实施例 1 的（27）相同（步骤 S207：第 3 次）。

（30）～（34）与实施例 1 同样（步骤 S210：第 3 次，步骤 S201：第 4 次，步骤 S211～S213）。

实施 2 的密码处理装置是将对前面信息但执行密码处理过程中生成的中间信息组作为链接信息组存贮，在后面的密码处理时组合进明文信息组和密码处理信息组，每次执行密码处理时更新该链结信息组。

15 <实施例 3>

本发明实施例 3 的数据加密装置 10，仅第 5 加密单元 105e 的输入与实施例 1 不同。实施例 1 中第 5 加密单元 105e 的输入为第 4 加密单元 105d 的输出，而在实施例 3 中该输入为明文信息组。因而，链结信息组和明文信息组分别由另外的加密单元处理。

20 本发明实施例 3 的数据译码装置 20 作为数据加密装置 10 的逆变换，与实施例 1 的数据译码装置 20 不同点是第 4 译码单元 205d 的输出为明文信息组，将对此明文信息组进行与数据加密装置 10 同样的加密处理生成的第 4 中间信息组作为新的链结信息组存贮。

密码通信系统的结构与实施例 1 相同，所以省略其说明。

25 图 16 表示本发明实施例 3 中图 2 所示数据加密装置 10 的详细结构。

与实施例 1 中图 3 所示数据加密装置 10 共同的构成部分加以同样的标号，具有同样功能的构成部分的说明省略。

此数据加密装置 10 的结构与实施例 1 相同，而仅在第 5 加密单元 105e 不由第 4 中间信息组而由明文信息组生成第 5 中间信息组这一点上与实施例 30 例 1 不同。

图 17 表示本发明实施例 3 中图 2 所示数据译码装置 20 的详细结构。

与实施例 1 中图 8 所示数据译码装置 20 共同的构成部分加以相同标号、具有同一功能的构成部分的说明省略。

此数据译码装置 20 由信息组分割单元 201、信息组存贮单元 202、关键数据组合单元 203、部分密钥生成单元 204、第 1~4 译码单元 205a~205d、第 1~4 加密单元 205i~205l、尾数数据处理单元 206 和信息组组合单元 207 构成。

第 4 译码单元 205d 根据第 5 部分密钥由第 5 中间信息组生成明文信息组。在此，由各自对应于第 1~3 密码文信息组的第 5 中间信息组生成第 1~3 明文信息组。而第 1~4 译码单元 205a~205d 进行的变换分别为数据加密装置 10 的第 8~5 加密单元 105h~105e 进行的变换的逆变换。

第 1 加密单元 205i 根据第 1 部分密钥由第 4 译码单元 205d 生成的明文信息组生成第 1 中间信息组。

第 2~4 加密单元 205j~205l 分别根据第 2~4 部分密钥由第 1~3 中间信息组生成第 2~4 中间信息组。

第 1~4 加密单元 205i~205l 各自具有与数据加密装置 10 的第 1~4 加密单元 105a~105d 同样的功能，其操作也完全相同。在此，由第 1~3 明文信息组生成各自对应的第 1~4 中间信息组。

信息组存贮单元 202 具有信息组更新功能，在每次第 4 加密单元 205l 生成第 4 中间信息组时，将此第 4 中间信息组作为新的链结信息组更新存贮中的链结信息组，在处理下一信息组时应用。这里的操作与实施例 1 相同。

信息组结合单元 207 将第 4 译码单元 205d 生成的明文数据的各信息组与尾数数据处理单元 206 生成的尾数明文数据相结合生成明文数据。在此将各 64 位的第 1~3 明文数据与 8 位的尾数明文数据相结合生成 200 位的明文数据。

图 18 表示本发明实施例 3 的数据加密装置 10 中的加密处理流程。

与实施例 1 中图 10 所示数据加密装置 10 的操作共同的步骤加以同样标号省略其说明。

(1) ~ (7) 与实施例 1 相同 (步骤 S101~S107: 第 1 次)。

(8)第5~7加密单元105e~105g分别根据第5~7的部分密钥由明文信息组和第5~6中间信息组生成第5~7中间信息组(步骤S501)。在此由第1明文信息组和对应于第1明文信息组的第5~6中间信息组生成第5~7中间信息组(步骤S501:第1次)。

5 (9)~(17)与实施例1相同(步骤S109、S110:第1次,步骤S101~S107:第2次)。

(18)在步骤S501中,这里由第2明文信息组和对应于第2明文信息组的第5~6中间信息组生成第5~7中间信息组(步骤S501:第2次)。

10 (19)~(27)与实施例1同样(步骤S109、S110:第2次,步骤S101~S107:第3次)。

(28)在步骤S501,这里由第3明文信息组和对应于第3明文信息组的第5~6中间信息组生成第5~7中间信息组(步骤S501:第3次)。

(29)~(34)与实施例1相同(步骤S109、S110:第3次,步骤S101:第4次,步骤S111~S113)。

15 图19表示本发明实施例3的数据译码装置20中的加密处理流程。数据译码装置20的操作为数据加密装置10的操作的逆变换。

与实施例1中图11所示数据译码装置20的操作共同的步骤加以相同标号,省略其说明。

(1)~(5)与实施例1相同(步骤S201~S205:第1次)。

20 (6)第2~4译码单元205b~205d各自根据第7~5部分密钥由第7~5中间信息组生成第6、第5中间信息组和明文信息组(步骤S601)。在此由对应于第1密码文信息组的第7~5中间信息组生成第6、第5中间信息组和第1明文信息组(步骤S601:第1次)。

25 (7)第1加密单元205i根据第1部分密钥由第4译码单元205d生成的明文信息组生成第1中间信息组(步骤S602)。在此由第1明文信息组生成第1中间信息组(步骤S602:第1次)。

30 (8)第2~4密码单元205j~205l各自根据第2~4部分密钥由第1~3中间信息组生成第2~4中间信息组(步骤S603)。在此由对应于第1明文信息组的第1~3中间信息组生成第2~4中间信息组(步骤S603:第1次)。

(9) 信息组存贮单元 202 将第 4 加密单元 2051 生成的第 4 中间信息组作为新链结信息组更新存贮中的链接信息组（步骤 S604）。在此更新为对应于第 1 明文信息组的第 4 中间信息组（步骤 S604：第 1 次）。

(10) ～ (15) 与实施例 1 相同（步骤 S210：第 1 次，步骤 S201～
5 S205：第 2 次）。

(16) 在步骤 S601，这里由对应于第 2 密码文信息组的第 7～5 中间信息组生成第 6、第 5 中间信息组和第 2 明文信息组（步骤 S601：第 2 次）。

(17) 在步骤 S602，这里由第 2 明文信息组生成第 1 中间信息组（步
10 骤 S602：第 2 次）。

(18) 在步骤 S603，这里由对应于第 2 明文信息组的第 1～3 中间信息组生成第 2～4 中间信息组（步骤 S603：第 2 次）。

(19) 步骤 S604，在此更新为对应于第 2 明文信息组的第 4 中间信息组（步骤 S604：第 2 次）。

15 (20) ～ (25) 与实施例 1 相同（步骤 S210：第 2 次，步骤 S201～S205：第 3 次）。

(26) 在步骤 S601，这里由对应于第 3 密码文信息组的第 7～5 中间信息组生成第 6、第 5 中间信息组和第 3 明文信息组（步骤 S601：第 3 次）。

20 (27) 在步骤 S602，这里由第 3 明文信息组生成第 1 中间信息组（步骤 S602：第 3 次）

(28) 在步骤 S603，这里由对应于第 3 明文信息组的第 1～3 中间信息组生成第 2～4 中间信息组（步骤 S603：第 3 次）。

(29) 在步骤 S604，在此更新为对应于第 3 明文信息组的第 4 中间
25 信息组（步骤 S604：第 3 次）。

(30) ～ (34) 与实施例 1 相同（步骤 S210：第 3 次，步骤 S201：第 4 次，步骤 S211～S213）。

实施例 3 的密码装置是将对前面信息组执行密码处理过程中生成的中间信息组作为链结信息组存贮，在后面的密码处理时组合进关键数据，
30 每次执行密码处理即更新该链接信息组。

实施例3中是对将链结信息组组合进关键数据的实施例1进行如上述的变更,但也可对将链结信息组组合进明文信息组和密码处理信息组的实施例2同样地进行如上述的变更。

- 这样的密码处理装置是将对前面信息组施行密码处理的过程中生成
5 的中间信息组作为链结信息组存贮,在后面的密码处理时组合到明文信息组和密码处理信息组,每次执行密码处理时更新该链结数据。

<实施例4>

- 本发明实施例4,面对实施例2进行如实施例3的变更时,倒转对组合的数据进行加密的第1~4加密单元与存贮链结信息组的信息组存贮单元
10 的序号,将组合后或组合前的信息组作为新的链结信息组存贮。

密码通信系统的结构与实施例1相同,省略其说明。

图20表示本发明实施例4中图2所示数据加密装置10的详细结构。

与实施例2中图12所示数据加密装置10共同的结构部分加以同一标号,具有同一功能的构成部分省略其说明。

- 15 此数据加密装置10由信息组分割单元101、信息组存贮单元102、部分密钥生成单元104、第1~8加密单元105a~105h、尾数数据处理单元106、信息组结合单元107和信息组组合单元108构成。

第1加密单元105a不由组合明文信息组而由信息组存贮单元102中存贮的链结信息组生成第1中间信息组。

- 20 第1~4加密单元105a~105d具有与实施2同样的功能。在此,由链结信息组生成各自对应的第1~3中间信息组和密码处理信息组。

- 信息组组合单元108将第4加密单元105d生成的密码处理信息组组合到明文信息组,生成第4中间信息组。在此,当处理第1明文信息组时,对由链结信息组的初始值IV生成的64位的第1密码处理信息组与64位的第1明文信息组进行各对应位的“异或”运算,而当处理第2~3明文
25 信息组时,对第1~2明文信息组处理时所生成的64位的第2~3密码处理信息组与64位的第2~3明文信息组进行各对应位的“异或”运算。

- 信息组存贮单元102具有信息组更新功能,每次信息组组合单元108生成第4中间信息组时,将此第4中间信息组作为新链结信息组更新存贮
30 中的链结信息组,用于下一信息组的处理中。这里,预先存贮有64位的

初始值 IV，此初始值 IV 被用于处理第 1 明文信息组中，将这一处理时所生成的第 4 中间信息组作为新链结信息组存贮。然后，第 1 明文信息组处理时被更新的链结信息组被用于处理第 2 明文信息组时，将此处理时所生成的第 4 中间信息组作为新链结信息组存贮。而后，第 2 明文信息组处理时所存贮的链结信息组用于处理第 3 明文信息组中，将此处理时生成的第 4 中间信息组作为新的链结信息组存贮。最后，第 3 明文信息组处理时被存贮的链结信息组被用于处理尾数明文数据中。

第 5~8 加密单元 105e~105h 具有与实施例 2 同样的功能。在此由第 4 中间信息组生成各自对应的第 5~7 中间信息组和第 1~3 密码文信息组。

尾数数据处理单元 106 由信息组分割单元 101 接收尾数明文数据，根据第 4 加密单元 105d 生成的密码处理信息组，由尾数明文数据生成与尾数明文数据位数相同的尾数密码数据，它包含数据匹配单元 106a 和尾数数据组合单元 106b。

数据匹配单元 106a 由第 4 加密单元 105d 生成的密码处理信息组生成与尾数明文数据同样位数的尾数密码处理数据。在此因尾数明文数据为 8 位，所以生成由第 4 加密单元 105d 生成的密码处理信息组的例如高 8 位构成的尾数密码处理数据。

尾数数据组合单元 106b 将尾数密码处理数据组合到尾数明文数据。这里，对 8 位的尾数密码处理数据与 8 位的尾数明文数据进行各对应位的“异或”运算，生成 8 位的尾数密码文数据。

尾数数据处理单元 106 也可以具有与实施例 2 同样的功能。

图 21 表示本发明实施例 4 中图 2 所示译码装置 20 的详细构成。

与实施例 2 中图 13 所示数据译码装置 20 共同的结构部分加以同一标号，具有同样功能的构成部分的说明省略。

此数据译码装置 20 由信息组分割单元 201、信息组存贮单元 202、部分密钥生成单元 204、第 1~4 译码单元 205a~205d、第 1~4 加密单元 205i~205l、尾数数据处理单元 206、信息组结合单元 207 和信息组组合单元 208 构成。

第 1 加密单元 205i 根据第 1 部分密钥由信息组存贮单元 202 中存贮

的链结信息组生成第 1 中间信息组。

第 2~4 加密单元 205j~205l 各自根据第 2、4 部分密钥由第 1~3 中间信息组生成第 2 中间信息组、第 3 中间信息组和密码处理信息组。

信息组组合单元 208 将第 4 加密单元 205l 生成的密码处理信息组合进第 4 译码单元 205d 生成的第 4 中间信息组，生成明文信息组。在此，当处理第 1 密码文信息组时，对由链结信息组的初始值 IV 生成的 64 位的第 1 密码处理信息组与由第 1 密码文信息组生成的 64 位的第 4 中间信息组进行各对应位的“异或”运算生成 64 位的第 1 明文信息组，而当处理第 2~3 密码文信息组时，对由在第 1~2 密码文信息组处理时所生成的链结信息组生成的 64 位的第 2~3 密码处理信息组与由第 2~3 密码文信息组生成的 64 位的各自的第 4 中间信息组进行各对应位的“异或”运算生成 64 位的第 2~3 明文信息组。

尾数数据处理单元 206 由信息组分割单元 201 接收尾数密码文数据，根据第 4 加密单元 205l 生成的密码处理信息组，由尾数密码文数据生成与尾数密码文数据相同位数的尾数明文数据，它包含数据匹配单元 206a 和尾数数据组合单元 206b。

数据匹配单元 206a 由第 4 加密单元 205l 生成的密码处理信息组生成与尾数密码文数据同样位数的尾数密码处理数据。这里，因尾数密码文数据为 8 位，故生成由第 4 加密单元 205l 生成的密码处理信息组的例如高 8 位构成的尾数密码处理数据。

尾数数据组合单元 206b 将尾数密码处理数据组合进尾数密码文数据。在此对 8 位的尾数密码处理数据与 8 位的尾数密码文数据进行各对应位的“异或”运算，生成 8 位的尾数明文数据。

尾数数据处理单元 206 也可以具有与实施例 2 同样的功能。

图 22 表示本发明实施例 4 的数据加密装置 10 中的加密处理流程。

与实施例 2 中图 14 所示数据加密装置 10 的操作共同的步骤加以同一标号，省略其说明。

(1)~(3) 与实施例 2 相同(步骤 S101、S102、S103: 第 1 次)。

(4) 第 1 加密单元 105a 根据第 1 部分密钥由信息组存贮单元 102 中存贮的链结信息组生成第 1 中间信息组(步骤 S701)。在此由链结信息

组初始值 IV 生成第 1 中间信息组（步骤 S701：第 1 次）。

（5）第 2~4 加密单元 105b~105d 各自根据第 2~4 部分密钥由第 1~3 中间信息组生成第 2、第 3 中间信息组和密码处理信息组（步骤 S702）。这里，由对应于链结信息组的初始值 IV 的第 1~3 中间信息组生成第 2、第 3 中间信息组和第 1 密码处理信息组（步骤 S702：第 1 次）。

（6）信息组组合单元 108 将密码处理信息组组合到明文信息组，生成第 4 中间信息组（步骤 S703）。在此对 64 位的第 1 密码处理信息组与 64 位的第 1 明文信息组进行各对应位的“异或”运算，生成 64 位的第 4 中间信息组（步骤 S703：第 1 次）。

10 （7）~（13）与实施例 2 相同（步骤 S107~S110：第 1 次，步骤 S101、S102、S301：第 2 次）。

（14）在步骤 S701，这里由第 1 明文信息组处理时生成的 64 位的链结信息组生成第 1 中间信息组（步骤 S701：第 2 次）。

15 （15）在步骤 S702，这里由第 1 明文信息组处理时生成的链结信息组所对应的第 1~3 中间信息组生成第 2、第 3 中间信息组和第 2 密码处理信息组（步骤 S702：第 2 次）。

（16）在步骤 S703，这里对 64 位的第 2 密码处理信息组与 64 位的第 2 明文信息组进行各对应位的“异或”运算，生成 64 位的第 4 中间信息组（步骤 S703：第 2 次）。

20 （17）~（23）与实施例 2 相同（步骤 S107~S110：第 2 次，步骤 S101、S102、S301：第 3 次）。

（24）在步骤 S701，这里由第 2 明文信息组处理时生成的 64 位的链结信息组生成第 1 中间信息组（步骤 S701：第 3 次）。

25 （25）在步骤 S702，这里由对应于第 2 明文信息组处理时所生产的链结信息组的第 1~3 中间信息组生成第 2、第 3 中间信息组和第 3 密码处理信息组（步骤 S702：第 3 次）。

（26）在步骤 S703，这里对 64 位的第 3 密码处理信息组与 64 位的第 3 明文信息组进行各对应位的“异或”运算，生成 64 位的第 4 中间信息组（步骤 S703：第 3 次）。

30 （27）~（34）与实施例 2 相同（步骤 S107~S110：第 3 次，步骤

S101: 第4次, 步骤S111~S113)。

图23表示本发明实施例4的数据译码装置20中的加密处理流程。

数据译码装置20的操作为数据加密装置10的操作的逆变换。

与实施例2中图15所示数据译码装置20的操作共同的步骤加以同一
5 标号, 省略其说明。

(1)~(5)与实施例2相同(步骤S201、S202、S401、S205、S206:
第1次)。

(6)第1加密单元205i根据第1部分密钥由信息组存贮单元202中
存贮的链结信息组生成第1中间信息组(步骤S801)。这里由链结信息
10 组的初始值IV生成第1中间信息组(步骤S801: 第1次)。

(7)第2~4加密单元205j~205l各自根据第2~4部分密钥中第1~
3中间信息组生成第2、第3中间信息组和密码处理信息组(步骤S802)。
在此, 由对应于链结信息组的初始值IV的第1~3中间信息组生成第2、
第3中间信息组和第1密码处理信息组(步骤S802: 第1次)。

15 (8)信息组组合单元208将密码处理信息组组合到第4中间信息组,
生成明文信息组(步骤S803)。在此对64位的第1密码处理信息组与对
应于第1密码文信息组的64位的第4中间信息组进行各对应位的“异或”
运算, 生成64位的第1明文信息组(步骤S803: 第1次)。

(9)~(15)与实施例2相同(步骤S207、S210: 第1次, 步骤
20 S201、S202、S401、S205、S206: 第2次)。

(16)在步骤S801, 这里由第1密码文信息组处理时生成的64位的
链结信息组生成第1中间信息组(步骤S801: 第2次)。

(17)在步骤S802, 这里由对应于第1密码文信息组处理时生成的
链接信息组的第1~3中间信息组生成第2、第3中间信息组和第二密码
25 处理信息组(步骤S802: 第2次)。

(18)在步骤S803, 这里对64位的第2密码处理信息组与对应于第
2密码文信息组的64位的第4中间信息组进行各对应位的“异或”运算,
生成64位的第2明文信息组(步骤S803: 第2次)。

(19)~(25)与实施例2相同(步骤S207、S210: 第2次, 步骤
30 S201、S202、S401、S205、S206: 第3次)。

(26) 在步骤 S801, 这里由第 2 密码文信息组处理时生成的 64 位的链接信息组生成第 1 中间信息组 (步骤 S801: 第 3 次)。

(27) 在步骤 S802, 这里由对应于第 2 密码文信息组处理时生成的链结信息组的第 1~3 中间信息组生成第 2、第 3 中间信息组和第 3 密码处理信息组 (步骤 S802: 第 3 次)。

(28) 在步骤 S803, 这里对 64 位的第 3 密码处理信息组与对应于第 3 密码文信息组的 64 位的第 4 中间信息组进行各对应位的“异或”运算生成 64 位的第 3 明文信息组 (步骤 S803: 第 3 次)。

(29) ~ (34) 与实施例 2 同样 (步骤 S207、S210: 第 3 次, 步骤 S201: 第 4 次, 步骤 S211~S213)。

实施例 4 的密码处理装置将在对前面信息组执行密码处理过程中生成的中间信息组作为链结信息组存贮, 在后面的密码处理时执行密码处理组合进明文信息组和密码处理信息组, 每次执行密码处理更新该链结数据。

15 <实施例 5>

本发明实施例 5 仅在不是以组合后或组合前的信息组作为新的链结信息组、而是将对链结信息组执行密码处理后的信息组作为新的链结信息组加以存贮这一点上与实施例 4 不同。

密码通信系统的构成与实施例 1 相同, 说明省略。

20 图 24 表示本发明实施例 5 中图 2 所示数据加密装置 10 的详细结构。
与实施例 2 中图 12 所示数据加密装置 10 共同的构成部分加以同一标号, 具有相同功能的构成部分的说明省略。

此数据加密装置 10 内信息组分割单元 101、信息组存贮单元 102、部分密钥生成单元 104、第 1~8 加密单元 105a~105h、尾数数据处理单元
25 106、信息组结合单元 107 和信息组组合单元 108 构成。

第 1 加密单元 105a 不是由组合明文信息组、而是由信息组存贮单元 102 中存贮的链结信息组生成第 1 中间信息组。

第 1~4 加密单元 105a~105d 具有与实施例 2 同样的功能。在此由链结信息组生成各自对应的第 1~4 中间信息组。

30 信息组组合单元 108 将第 4 加密单元 105d 生成的第 4 中间信息组组

合进明文信息组，生成组合明文信息组。这里，在处理第1明文信息组时对由链结信息组的初始值IV生成的64位的第4中间信息组与64位的第1明文信息组进行各对应位的“异或”运算，而在处理第2~3明文信息组时对第1~2明文信息组处理时生成的各自对应的64位的第4中间信息组与64位的第2~3明文信息组进行各对应位的“异或”运算。

第5加密单元105e不是由第4中间信息组、而是由信息组组合单元108生成的组合明文信息组生成第5中间信息组。

第5~8加密单元105e~105h具有与实施例2同样的功能。在此，由组合明文信息组生成各自对应的第5~7中间信息组和第1~3密码文信息组。

尾数数据处理单元106具有与实施例4同样的功能。

尾数数据处理单元106也可以与实施例2具有同样的功能。

图25表示本发明实施例5中图2所示数据译码装置20的详细结构。

与实施例2中图13所示数据译码装置20共同的构成部分加以相同标号，具有同一功能的构成部分的说明省略。

此数据译码装置20由信息组分割单元201、信息组存贮单元202、部分密钥生成单元204、第1~4译码单元205a~205d、第1~4加密单元205i~205l、尾数数据处理单元206、信息组结合单元207和信息组组合单元208构成。

第4译码单元205d根据第5部分密钥由第5中间信息组生成密码处理信息组。在此，由各自对应于第1~3密码文信息组的第5中间信息组生成第1~3密码处理信息组。第1~4译码单元205a~205d进行的变换各自为数据加密装置10的第4~1加密单元105d~105a进行的变换的逆变换。

第1加密单元205i根据第1部分密钥由信息组存贮单元202中存贮的链结信息组生成第1中间信息组。

第2~4加密单元205j~205l各自根据第2~4部分密钥由第1~3中间信息组生成第2~4中间信息组。

信息组存贮单元202具有信息组更新功能，每次第4加密单元205l生成第4中间信息组时，将此第4中间信息组作为新链结信息组更新存贮

中的链结信息组，用于处理下一信息组中。这里的操作与实施例 1 相同。

第 1~4 加密单元 205i~205l 各自具有与数据加密装置 10 的第 1~4 加密单元 105a~105d 同一的功能，其操作也完全相同。在此，由各链结信息组各自生成对应的第 1~4 中间信息组。

- 5 信息组组合单元 208 将第 4 加密单元 205l 生成的第 4 中间信息组组合进第 4 译码单元 205d 生成的密码处理信息组，生成明文信息组。这里，在处理第 1 密码文信息组时，对由链结信息组的初始值 IV 生成的 64 位的第 4 中间信息组与由第 1 密码文信息组生成的 64 位的密码处理信息组进行各对应位的“异或”运算，生成 64 位的第 1 明文信息组，而在处理第 10 2~3 密码文信息组时对由第 1~2 密码文信息组处理时生成的链结信息组生成的 64 位的各自的第 4 中间信息组与由第 2~3 密码文信息组生成的 64 位的第 2~3 密码处理信息组进行各对应位的“异或”运算，生成 64 位的第 2~3 明文信息组。

尾数数据处理单元 206 具有与实施例 4 的同一的功能。

- 15 尾数数据处理单元 206 也可以具有与实施例 2 的同样功能。

图 26 表示本发明实施例 5 的数据加密装置 10 中的加密处理流程。

与实施例 2 中的图 14 所示数据加密装置 10 的操作共同的步骤加以同一标号，其说明省略。

(1) ~ (3) 与实施例 2 相同（步骤 S101、S102、S301：第 1 次）。

- 20 (4) 第 1 加密单元 105a 根据第 1 部分密钥由信息组存贮单元 102 中存贮的链结信息组生成第 1 中间信息组（步骤 S901）。在此，由链结信息组的初始值 IV 生成第 1 中间信息组（步骤 S901：第一次）。

(5) ~ (6) 与实施例 2 的 (6) ~ (7) 相同（步骤 S106、S107：第一次）。

- 25 (7) 信息组组合单元 108 将第 4 中间信息组组合进明文信息组，生成组合明文信息组（步骤 S902）。这里，对与链结信息组的初始值 IV 相对应的 64 位的第 4 中间信息组与 64 位的第 1 明文信息组进行各对应位的“异或”运算生成 64 位的第 1 组合明文信息组（步骤 S902：第 1 次）。

- 30 (8) 第 5 加密单元 105e 根据第 5 部分密钥由组合明文信息组生成第 5 中间信息组，第 6~7 加密单元 105f~105g 各自根据第 6~7 部分密钥由

第5~6中间信息组生成第6~7中间信息组（步骤S903）。这里由第1组合明文信息组生成第5中间信息组，由5~6中间信息组生成第6~7中间信息组（步骤S903：第1次）。

（9）~（13）与实施例2同样（步骤S109、S110：第1次，步骤S101、S102、S301：第2次）。

（14）在步骤S901，这里由第1明文信息组处理时生成的64位的链结信息组生成第1中间信息组（步骤S901：第2次）。

（15）~（16）与实施例2的（16）~（17）同样（步骤S106、S107：第2次）。

10 （17）在步骤S902，这里对与第1明文信息组处理时生成的链结信息组相对应的64位的第4中间信息组与64位的第2明文信息组进行各对应位的“异或”运算生成64位的第2组合明文信息组（步骤S902：第2次）。

（18）在步骤S903，这里由第2组合明文信息组生成第5中间信息组，由5~6中间信息组生成第6~7中间信息组（步骤S903：第2次）。

15 （19）~（23）与实施例2相同（步骤S109、S110：第2次，步骤S101、S102、S301：第3次）。

（24）步骤S901中，这里由第2明文信息组处理时生成的64位的链结信息组生成第1中间信息组（步骤S901：第3次）。

20 （25）~（26）与实施例2的（26）~（27）相同（步骤S106、S107：第3次）。

（27）在步骤S902，这里对与第2明文信息组处理时所生成的链结信息组相对应的64位的第4中间信息组与64位的第3明文信息组进行各对应位的“异或”运算生成64位的第3组合明文信息组（步骤S902：第25 3次）。

（28）在步骤S903，在此由第3组合明文信息组生成第5中间信息组，由5~6中间信息组生成第6~7中间信息组（步骤S903：第3次）。

（29）~（34）与实施例2相同（步骤S109~S110：第3次，步骤S101：第4次，步骤S111~S113）。

30 图27表示本发明实施例5的数据译码装置20中的加密处理流程。

数据译码装置 20 的操作为数据加密装置 10 的操作的逆变换。

与实施例 2 中图 15 所示数据译码装置 20 的操作共同的步骤加以同一标号，其说明省略。

(1) ~ (4) 与实施例 2 同样（步骤 S201、S202、S401、S205：第 5 1 次）。

(5) 第 2~4 译码单元 205b~205d 分别根据第 7~5 部分密钥由第 7~5 中间信息组生成第 6、第 5 中间信息组和密码处理信息组（步骤 S1001）。在此，由对应于第 1 密码文信息组的第 7~5 中间信息组生成第 6、第 5 中间信息组和第 1 密码处理信息组（步骤 S1001：第 1 次）。

10 (6) 第 1 加密单元 20ri 根据第 1 部分密钥由信息组存贮单元 202 中存贮的链结信息组生成第 1 中间信息组（步骤 S1002）。在此，由链结信息组的初始值 IV 生成第 1 中间信息组（步骤 S1002：第 1 次）。

(7) 第 2~4 加密单元 205j~205l 各自根据第 2~4 部分密钥由第 1~3 中间信息组生成第 2~4 中间信息组（步骤 S1003）。在此由对应于链结
15 信息组的初始值 IV 的第 1~3 中间信息组生成第 2~4 中间信息组（步骤 S1003：第 1 次）。

(8) 信息组组合单元 208 将第 4 中间信息组组合到密码处理信息组生成明文信息组（步骤 S1004）。在此，对与第 1 密码文信息组相对应的 64 位的第 4 中间信息组与 64 位的第 1 密码处理信息组进行各对应位的“异
20 或”运算生成 64 位的第 1 明文信息组（步骤 S1004：第 1 次）。

(9) ~ (14) 与实施例 2 相同（步骤 S207、S210：第 1 次，步骤 S201、S202、S401、S205：第 2 次）。

(15) 在步骤 S1001，这里由对应于第 2 密码文信息组的第 7~5 中间信息组生成第 6、第 5 中间信息组和第 2 密码处理信息组（步骤 S1001：
25 第 2 次）。

(16) 在步骤 S1002，这里由第 1 密码文信息组处理时的生成的 64 位的链结信息组生成第 1 中间信息组（步骤 S1002：第 2 次）。

(17) 在步骤 S1003，这里由对应于第 1 密码文信息组处理时所生成的链结信息组的第 1~3 中间信息组生成第 2~4 中间信息组（步骤
30 S1003：第 2 次）。

(18) 在步骤 S1004: 这里对与第 2 密码文信息组相对应的 64 位的第 4 中间信息组与 64 位的第 2 密码处理信息组进行各对应位的“异或”运算生成 64 位的第 2 明文信息组 (步骤 S1004: 第 2 次)。

(19) ~ (24) 与实施例 2 相同 (步骤 S207、S210: 第 2 次, 步骤 S201、S202、S401、S205: 第 3 次)。

(25) 步骤 S1001 中, 这里由对应于第 3 密码文信息组的第 7~5 中间信息组生成第 6、第 5 中间信息组和第 3 密码处理信息组 (步骤 S1001: 第 3 次)。

(26) 步骤 S1002 中, 这里由第 2 密码文信息组处理时所生成的 64 位链结信息组生成第 1 中间信息组 (步骤 S1002: 第 3 次)。

(27) 步骤 S1003 中, 这里由对应于第 2 密码文信息组处理时生成的链结信息组的第 1~3 中间信息组生成第 2~4 中间信息组 (步骤 S1003: 第 3 次)。

(28) 步骤 S1004 中, 在此对与第 3 密码文信息组相对应的 64 位的第 4 中间信息组与 64 位的第 3 密码处理信息组进行各对应位的“异或”运算, 生成 64 位的第 3 明文信息组 (步骤 S1004: 第 3 次)。

(29) ~ (24) 与实施例 2 同样 (步骤 S207、S210: 第 3 次, 步骤 S201: 第 4 次, 步骤 S211~S213)。

实施例 5 的密码处理装置将对前面信息组进行密码处理过程中生成的中间信息组作为链结信息组存贮, 在后面的密码处理时执行密码处理组合进明文信息组和密码处理信息组, 每次执行密码处理时更新该链结信息组。

本发明的实施例 6 为执行由关键数据指定的密码处理、由被作密码处理数据生成输出数据的密码处理装置, 以信息组为单位在每次执行密码处理时将输出信息组、被作密码处理信息组和中间信息组等作为链结信息组加以存贮, 在进行下一信息组的密码处理时对存贮中的链结信息组进行信息组变换组合到关键数据。

密码通信系统的结构因与实施例 1 相同, 故说明省略。

图 28 表示本发明实施例 6 中图 2 所示数据加密装置 10 的详细构成。与实施例 1 中图 3 所示数据加密装置 10 共同的结构部分加以同一标

号，具有同样功能的构成部分说明省略。

此数据加密装置 10 由信息组分割单元 101、信息组存贮单元 102、关键数据组合单元 103、部分密钥生成单元 104、第 1~8 加密单元 105a~105h、尾数数据处理单元 106、信息组结合单元 107 和信息组变换单元 109 5 构成。

信息组存贮单元 102 具有信息组更新功能，每次第 8 加密单元 105h 生成密码文信息组时，将此密码文信息组作为新链结信息组更新存贮着的链结信息组，用于处理下一信息组。这里，预先存贮 64 位的初始值 IV，将此初始值 IV 用于处理第 1 明文信息组，将此处理时所生成的第 1 密码文信息组更新为新链结信息组。再将第 1 明文信息组处理时更新的链结信息组用于第 2 明文信息组的处理，将此处理时所生成的第 2 密码文信息组更新为新链结数据。然后第 2 明文信息组处理时更新的链结信息组在处理第 3 明文信息组时应用，将此处理中生成的第 3 密码文信息组更新为新的链结信息组。最后，第 3 明文信息组处理时更新的链结信息组在处理尾数 15 明文数据时加以利用。

信息组变换单元 109 对信息组存贮单元 102 中存贮的链结信息组执行预先确定的规定变换生成变换信息组。这里，信息组变换单元 109 执行的规定变换，例如是位置换和位变换等。这种所谓的位置换是与实施例 1 的第 1~8 加密单元 105a~105h 中说明的转置 P 同样的以位为单位的置 20 换，而所谓的位变换则是与特定数据进行“异或”运算等的固定位单位的运算。这里，在处理第 1 明文信息组时，由 64 位的链结信息组的初始值 IV 生成 64 位的第 1 变换信息组，而在处理第 2~3 明文信息组时则由第 1~2 明文信息组处理时各自生成的 64 位的链结信息组生成 64 位的第 2~3 变换信息组。

25 关键数据组合单元 103 将信息组变换单元 109 生成的变换信息组合到关键数据生成组合关键数据。在此，预先获取所设定的 64 位的关键数据，在处理第 1 明文信息组时对 64 位的第 1 变换信息组与 64 位的关键数据进行各对应位的“异或”运算，而在处理第 2~3 明文信息组时对 64 位的第 2~3 变换信息组与 64 位的关键数据进行各对应位的“异或”运算。

30 尾数数据处理单元 106 由信息组分割单元 101 接收尾数明文数据，根

据信息组变换单元 109 生成的变换信息组,由尾数明文数据生成与尾数明文数据位数相同的尾数密码文数据,它包含数据匹配单元 106a 和尾数数据组合单元 106b。

数据匹配单元 106a 由信息组变换单元 109 生成的变换信息组生成与尾数明文数据相同位数的尾数变换数据。在此,因尾数明文数据为 8 位,所以生成由信息组变换单元 109 生成的变换信息组的例如高 8 位构成的尾数变换数据。

尾数数据组合单元 106b 将尾数变换数据组合到尾数明文数据。在此对 8 位的尾数变换数据与 8 位的尾数明文数据进行各对应位的“异或”运算生成 8 位的尾数密码文数据。

尾数数据处理单元 106 也可以具有与实施例 1 同样功能。

图 29 表示本发明实施例 6 中图 2 所示数据译码装置 20 的详细构成。

与实施例 1 中图 8 所示译码装置 20 共同的构成部分加以同一标号,具有同样功能的结构部分的说明省略。

此数据译码装置 20 由信息组分割单元 201、信息组存贮单元 202、关键数据组合单元 203、部分密钥生成单元 204、第 1~8 译码单元 205a~205h、尾数数据处理单元 206、信息组结合单元 207 和信息组变换单元 209 构成。

信息组存贮单元 202 具有信息组更新功能,每次信息组分割单元 201 生成密码文信息组时,即将此密码文信息组作为新链结信息组更新存贮中链结信息组,用于处理下一信息组。在此,预先存贮 64 位的初始值 IV,此初始值 IV 被用于处理第 1 密码文信息组,将第 1 密码文信息组作为新链结信息组存贮。再将第一密码文信息组处理时被更新的链结信息组用于处理第 2 密码文信息组,将第 2 密码文信息组作为新的链结信息组存贮。然后,第 2 密码文信息组处理时存贮的链结信息组被用于处理第 3 密码文信息组,将第 3 密码文信息组作为新链结信息组存贮。最后,第 3 密码文信息组处理时所存贮的链结信息组在处理尾数密码文数据时应用。

信息组变换单元 209 对信息组存贮单元 202 中存贮的链结信息组进行预先确定的规定变换生成变换信息组。这里,信息组变换单元 209 执行的规定变换与数据译码装置 10 的信息组变换单元 109 执行的规定变换相

同, 例如位置换和位变换等。在此, 当处理第 1 密码文信息组时由 64 位的链结信息组的初始值 IV 生成 64 位的第 1 变换信息组, 而当处理第 2~3 密码文信息组时则由第 1~2 密码文信息组处理时分别生成的 64 位的链结信息组生成 64 位的第 2~3 变换信息组。

5 关键数据组合单元 203 将信息组变换单元 209 生成的变换信息组组合到关键数据生成组合关键数据。这里, 获取预先设定的 64 位的关键数据, 在处理第 1 密码文信息组时对 64 位的第 1 变换信息组与 64 位的关键数据进行各对应位的“异或”运算, 而在处理第 2~3 密码文信息组时对 64 位的第 2~3 变换信息组与 64 位的关键数据进行各对应位的“异或”运算。

10 尾数数据处理单元 206 由信息组分割单元 201 接收尾数密码文数据, 根据信息组变换单元 109 生成的变换信息组由尾数密码文数据生成与尾数密码文数据相同位数的尾数明文数据, 它含有数据匹配单元 206a 和尾数数据组合单元 206b。

15 数据匹配单元 206a 由信息组变换单元 109 生成的变换信息组, 生成与尾数密码文数据相同位数的尾数变换数据。这里, 尾数密码文数据为 8 位, 故生成由信息组变换单元 109 生成的变换信息组的例如高 8 位构成的尾数变换数据。

20 尾数数据组合单元 206b 将尾数变换数据组合到尾数密码文数据。在此, 对 8 位的尾数变换数据与 8 位的尾数密码文数据进行各对应位的“异或”运算生成 8 位的尾数明文数据。

尾数数据处理单元 206 也可以具有与实施例 1 同样的功能。

图 30 表示本发明实施例 6 的数据密码文装置 10 中的加密处理流程。

与实施例 1 中图 10 所示数据加密装置 10 的操作共同的步骤加以同一标号, 其说明省略。

25 (1) ~ (2) 与实施例 1 相同 (步骤 S101、S102: 第 1 次)。

30 (3) 信息组变换单元 109 对信息组存贮单元 102 中存贮的链结信息组进行预先确定的规定变换生成变换信息组, 关键数据组合单元 103 将该变换信息组组合到关键数据生成组合关键数据 (步骤 S1101)。在此, 由 64 位的链结信息组的初始值 IV 生成 64 位的第 1 变换信息组, 获取预设的 64 位的关键数据, 对 64 位的第 1 变换信息组与 64 位的关键数据进行

各对应位的“异或”运算（步骤 S1101：第 1 次）。

（4）～（8）与实施例 1 的（4）～（6）、（8）、（9）相同（步骤 S104～S106、S108、S109：第 1 次）。

（9）信息组存贮单元 102 将密码文信息组作为新的链结信息组更新
5 存贮中的链结信息组（步骤 S1102）。在此，更新为第 1 密码文信息组（步骤 S1102：第 1 次）。

（10）～（12）与实施例 1 相同（步骤 S110：第 1 次，步骤 S101、S102：第 2 次）。

（13）在步骤 S1101，这里，由第 1 明文信息组处理时所生成的 64
10 位的链结信息组生成 64 位的第二变换信息组，对此 64 位的第 2 变换信息组与 64 位的关键数据进行各对应位的“异或”运算（步骤 S1101：第 2 次）。

（14）～（18）与实施例 1 的（14）～（16）、（18）、（19）相同（步骤 S104～S106、S108、S109：第 2 次）。

15 （19）步骤 S1102 中，这里更新为第 2 密码文信息组（步骤 S1102：第 2 次）。

（20）～（22）与实施例 1 相同（步骤 S110：第 2 次，步骤 S101、S102：第 3 次）。

（23）步骤 S1101 中，这里由第 2 明文信息组处理时所生成的 64 位
20 的链结信息组生成 64 位的第 3 变换信息组，对此 64 位的第 3 变换信息组与 64 位的关键数据进行各对应位的“异或”运算（步骤 S1101：第 3 次）。

（24）～（28）与实施例 1 的（24）～（26）、（28）、（29）相同（步骤 S104～S106、S108、S109：第 3 次）。

25 （29）在步骤 S1102，这里更新为第 3 密码文信息组（步骤 S1102：第 3 次）。

（30）～（34）与实施例 1 相同（步骤 S110：第 3 次，S101：第 4 次，S111～S113）。

图 31 表示本发明实施例 6 的数据译码装置 20 中的加密处理流程。

数据译码装置 20 的操作为数据加密装置 10 的操作的逆变换。

30 与实施例 1 中图 11 所示数据译码装置 20 的操作共同的步骤加以同一

标号，其说明省略。

(1) ~ (2) 与实施例 1 相同 (步骤 S201、S202: 第 1 次)。

(3) 信息组变换单元 209 对信息组存贮单元 202 中存贮的链结信息组进行预先确定的规定变换生成变换信息组, 关键数据组合单元 203 将该
5 变换信息组组合到关键数据生成组合关键数据 (步骤 S1201)。在此, 由 64 位的链结信息组的初始值 IV 生成 64 位的第 1 变换信息组, 获取预设的 64 位的关键数据, 对此 64 位的第 1 变换信息组与 64 位的关键数据进行各对应位的“异或”运算 (步骤 S1201: 第 1 次)。

(4) ~ (8) 与实施例 1 的 (4) ~ (6)、(8)、(9) 相同 (步骤
10 S204~S206、S208、S209: 第 1 次)。

(9) 信息组存贮单元 202 将密码文信息组作为新链结信息组更新存贮中的链结信息组 (步骤 1202)。在此更新为第 1 密码文信息组 (步骤 1202: 第 1 次)。

(10) ~ (12) 与实施例 1 相同 (步骤 S210: 第 1 次, S201、S202:
15 第 2 次)。

(13) 在步骤 S1201, 这里由第 1 明文信息组处理时生成的 64 位的链结信息组生成 64 位的第 2 变换信息组, 对此 64 位的第 2 变换信息组与 64 位的关键数据进行各对应位的“异或”运算 (步骤 S1201: 第 2 次)。

(14) ~ (18) 与实施例 1 的 (14) ~ (16)、(18)、(19) 相同
20 (步骤 S204~S206、S208、S209: 第 2 次)。

(19) 在步骤 S1202, 这里更新为第 2 密码文信息组 (步骤 S1202: 第 2 次)。

(20) ~ (22) 与实施例 1 同样 (步骤 S210, 第 2 次, S201、S202: 第 3 次)。

(23) 在步骤 1201, 这里由第 22 明文信息组处理时所生成的 64 位的链结信息组生成 64 位的第 3 变换信息组, 对此 64 位的第 3 变换信息组与 64 位的关键数据进行各对应位的“异或”运算 (步骤 S1201: 第 3 次)。

(24) ~ (28) 与实施例 1 的 (24) ~ (26)、(28)、(29) 相同 (步骤 S204~S206、S209、S209: 第 3 次)。

(29) 步骤 S1202 中, 在此更新为第 3 密码文信息组 (步骤 S1202:
30

第3次)。

(30)~(34)与实施例1同样(步骤S210:第3次,S201:第4次,S211~S213)。

实施例6的密码处理装置将前面的密码文信息组作为链结信息组存
5 贮,在后面的密码处理时执行信息组变换组合到关键数据,每次进行密码处理时更新该链结信息组。

上述实施例6虽然将密码文信息组作为新链结信息组,但也可以将明文信息组或任何的中间信息组作为新的链结信息组。

<实施例7>

10 本发明实施例7与实施例6不同之处是,不是将对链结信息组进行信息组变换的变换信息组合到关键数据,而是组合到被作密码处理数据或对被作密码处理数据执行密码处理后的数据。

密码通信系统的构成与实施例1同样,其说明省略。

图32表示本发明实施例7中图2所示数据加密装置10的详细结构。

15 与实施例2中图12所示数据加密装置10共同的构成部分加以同一标号,具有同样功能的结构部分的说明省略。

此数据加密装置10由信息组分割单元101、信息组存贮单元102、部分密钥生成单元104、第1~8加密单元105a~105h、尾数数据处理单元106、信息组结合单元107、信息组组合单元108和信息组变换单元109
20 构成。

信息组存贮单元102具有信息组更新功能,每次第8加密单元105h生成密码文信息组时,将此密码文信息组作为新的链结信息组更新存贮中的链结信息组,用于处理下一信息组。这里,预先存贮64位的初始值IV,此初始值IV用于处理第1明文信息组,将此处理时所生成的第1密码文
25 信息组更新为新连结信息组。此第1明文信息组处理时更新的链结信息组再在处理第2明文信息组时加以利用,将此处理时生成的第2密码文信息组更新为新的链结信息组。然后,第2明文信息组处理时更新的链结信息组在处理第3明文信息组时应用,将此处理时所生成的第3密码文信息组更新为新的链结信息组。最后,在第3明文信息组处理时更新的链结信息
30 组被用于尾数明文数据处理。

信息组变换单元 109 对信息组存贮单元 102 中存贮的链结信息组进行预先确定的规定变换生成变换信息组。这里，信息组变换单元 109 执行的规定变换例如为位置换和位变换等。此所谓位置换为与实施例 1 的第 1~8 密码文单元 105a~105h 中说明的转置 P 同样的以位为单位的置换，所谓位变换是与特定的数据进行“异或”运算等的固定的位单位的运算。这里，在处理第 1 明文信息组时，由 64 位的链结信息组的初始值 IV 生成 64 位的第 1 变换信息组，而在处理第 2~3 明文信息组时，由第 1~2 明文信息组处理时分别生成的 64 位的链结信息组生成 64 位的第 2~3 变换信息组。

10 信息组组合单元 108 将信息组变换单元 109 生成的变换信息组组合到明文信息组生成组合明文信息组。这里，在处理第 1 明文信息组时，对 64 位的第 1 变换信息组与 64 位的第 1 明文信息组进行各对应位的“异或”运算生成 64 位的第 1 组合明文信息组，而在处理第 2~3 明文信息组时，对 64 位的第 2~3 变换信息组与 64 位的第 2~3 明文信息组进行各对应位的“异或”运算生成 64 位的第 2~3 组合明文信息组。

图 33 表示本发明实施例 7 中图 2 所示数据译码装置 20 的详细结构。

与实施例 2 中图 13 所示数据译码装置 20 共同的构成部分加以同一标号，具有同样功能的构成部分的说明省略。

20 此数据译码装置 20 由信息组分割单元 201、信息组存贮单元 202、关键数据组合单元 203、部分密钥生成单元 204、第 1~8 译码单元 205a~205h、尾数数据处理单元 206、信息组结合单元 207 和信息组变换单元 209 构成。

25 信息组存贮单元 202 具有信息组更新功能，每次信息组分割单元 201 生成密码文信息组时，将此密码文信息组作为新链结信息组更新存贮中的链结信息组，在处理下一信息组时应用。这里，预先存贮 64 位的初始值 IV，此初始值 IV 在处理第 1 密码文信息组时应用，将此第 1 密码文信息组作为新链结信息组存贮。接着，第 1 密码文信息组处理时所更新的链结信息组被用于处理第 2 密码文信息组，并将第 2 密码文信息组作为新链结信息组存贮。然后，第 2 密码文信息组处理时存贮的链结信息组用于处理 30 第 3 密码文信息组，将第 3 密码文信息组作为新链结信息组存贮。最后，

第3密码文信息组处理时存贮的链结信息组用于尾数密码文数据的处理。

信息组变换单元209对信息组存贮单元202中存贮的链结信息组进行预先确定的规定变换,生成变换信息组。这里,信息组变换单元209执行的规定变换与数据加密装置10的信息组变换单元109所执行的规定变换相同,例如位置换和位变换等。这里,在处理第1密码文信息组时由64位的链结信息组的初始值IV生成64位的第1变换信息组,而在处理第2~3密码文信息组时由第1~2密码文信息组处理时分别生成的64位的链结信息组生成64位的第2~3变换信息组。

10 信息组组合单元208将信息组变换单元209生成的变换信息组组合到密码处理信息组,生成明文信息组。这里,在处理第1密码文信息组时对64位的第1变换信息组与64位的第1密码处理信息组进行各对应位的“异或”运算生成64位的第1明文信息组,而在处理第2~3密码文信息组时对64位的第2~3变换信息组与64位的第2~3密码处理信息组进行各对应位的“异或”运算生成64位的第2~3明文信息组。

图34表示本发明实施例7的数据加密装置10的加密处理流程。

与实施例2中图14所示数据加密装置10的操作共同的步骤加以同一标号,其说明省略。

(1)~(3)与实施例2相同(步骤S101、S102、S301:第1次)。

20 (4)信息组变换单元109对信息组存贮单元102中存贮的链结信息组进行预先确定的规定变换生成变换信息组,信息组组合单元108将该变换信息组组合到明文信息组生成组合明文信息组(步骤S1301)。这里,由64位的链结信息组的初始值IV生成64位的第1变换信息组,对此64位的第1变换信息组与64位的第1明文信息组进行各对应位的“异或”运算,生成64位的第1组合明文信息组(步骤S1301:第1次)。

25 (5)~(8)与实施例2相同(步骤S303、S106、S108、S109:第1次)。

(9)信息组存贮单元102将密码文信息组作为新链结信息组更新存贮中的链接信息组(步骤S1302)。这里,更新为第1密码文信息组(步骤S1302:第1次)。

(10) ~ (13) 与实施例 2 相同 (步骤 S110: 第 1 次, S101、S102、S301: 第 2 次)。

(14) 在步骤 S1301, 这里, 由第 1 明文信息组处理时所生成的 64 位的链结信息组生成 64 位的第 2 变换信息组, 对此 64 位的第 2 变换信息组与 64 位的第 2 明文信息组进行各对应位的“异或”运算, 生成 64 位的第 2 组合明文信息组 (步骤 S1301: 第 2 次)。

(15) ~ (18) 与实施例 2 相同 (步骤 S303、S106、S108、S109: 第 2 次)。

(19) 在步骤 S1302, 这里更新为第 2 密码文信息组 (步骤 S1302: 第 2 次)。

(20) ~ (23) 与实施例 2 相同 (步骤 S110: 第 2 次, S101、S102、S301: 第 3 次)。

(24) 步骤 S1301, 在此由第 2 明文信息组处理时所生成的 64 位的链结信息组生成 64 位的第 3 变换信息组, 对此 64 位的第 3 变换信息组与 64 位的第 3 明文信息组进行各对应位的“异或”运算, 生成 64 位的第 3 组合明文信息组 (步骤 S1301: 第 3 次)。

(25) ~ (28) 与实施例 2 同样 (步骤 S303、S106、S108、S109: 第 3 次)。

(29) 在步骤 S1302, 这里更新为第 3 密码文信息组 (步骤 S1302: 第 3 次)。

(30) ~ (34) 与实施例 2 同样 (步骤 S110: 第 3 次, S101: 第 4 次, S111~S113)。

图 35 表示本发明实施例 7 的数据译码装置 20 中的加密处理流程。

数据译码装置 20 的操作为数据加密装置 10 的操作的逆变换。

与实施例 2 中图 15 所示数据译码装置 20 的操作共同的步骤加以同一标号, 其说明省略。

(1) ~ (7) 与实施例 1 相同 (步骤 S201~S202、S401、S205、S206、S208、S402: 第 1 次)。

(8) 信息组变换单元 209 对信息组存贮单元 202 中所存贮的链结信息组进行预先确定的规定变换生成变换信息组, 信息组组合单元 208 将该

变换信息组组合到密码处理信息组生成明文信息组（步骤 S1401）。在此，由链结信息组的初始值 IV 生成 64 位的第 1 变换信息组，对此 64 位的第 1 变换信息组和 64 位的第 1 密码处理信息组进行各对应位的“异或”运算生成 64 位的第 1 明文信息组（步骤 S1401：第 1 次）。

- 5 （9）信息组存贮单元 202，将密码文信息组作为新链结信息组更新存贮中的链结信息组（步骤 S1402：第 1 次）。

 （10）～（17）与实施例 1 相同（步骤 S210：第 1 次，S201、S202、S401、S205、S206、S208、S402：第 2 次）。

- 10 （18）在步骤 S1401，这里，由第 1 明文信息组处理时所生成的 64 位的链结信息组生成 64 位的第 2 变换信息组，对此 64 位的第 2 变换信息组与 64 位的第 2 密码处理信息组进行各对应位的“异或”运算，生成 64 位的第 2 明文信息组（步骤 S1401：第 2 次）。

 （19）在步骤 S1402，这里更新为第 2 密码文信息组（步骤 S1402：第 2 次）。

- 15 （20）～（27）与实施例 1 相同（步骤 S210：第 2 次，S201、S202、S401、S205、S206、S208、S402：第 3 次）。

- （28）在步骤 S1401，这里由第 2 明文信息处理时所生成的 64 位的链结信息组生成 64 位的第 3 变换信息组，对此 64 位的第 3 变换信息组与 64 位的第 3 密码处理信息组进行各对应位的“异或”运算，生成 64 位的
20 第 3 明文信息组（步骤 S1401：第 3 次）。

 （29）在步骤 S1402，这里更新为第 3 密码文 信息组（步骤 S1402：第 3 次）。

 （30）～（34）与实施例 1 相同（步骤 S210：第 3 次，S201：第 4 次，S211～S213）。

- 25 实施例 7 的密码处理装置，将前面的密码文信息组作为链结信息组存贮，在后面的密码处理时进行信息组变换组合进明文信息组和密码处理信息组，每次进行密码处理时更新该链结信息组。

 在上述实施例 7 中虽是以密码文信息组作为新链结信息组，但也可将明文信息组或任何一个中间信息组作为新链结信息组。

- 30 <实施例 8>

本发明实施例 8 的数据加密装置 10, 在第 1 加密单元 105a、信息组存贮单元 102、信息组结合单元 107 和信息组组合单元 108 的各个输入上与实施例 7 不同, 处理顺序替换。

本发明实施例 8 的数据译码装置 20, 仅信息组存贮单元的输入与数
5 加密装置 10 的不同这一点之外, 均与数据加密装置 10 相同。

密码通信系统的结构与实施例 1 相同, 说明省略。

图 36 表示本发明实施例 8 中图 2 所示数据加密装置 10 的详细结构。

与实施例 7 中图 32 所示数据加密装置 10 共同的结构部分加以同一标号, 具有相同功能的结构部分说明省略。

10 此数据加密装置 10 的结构与实施例 7 相同。

第 1 加密单元 105a 不是如实施例 7 那样由信息组组合单元 108 生成的组合明文信息组、而是由信息组变换单元 109 生成的变换信息组生成第 1 中间信息组。

第 8 加密单元 105h 不是如实施例 7 那样的密码文信息组、而是生成
15 密码处理信息组。

第 1~8 加密单元 105a~105h 具有与实施例 7 同样的功能。这里, 由第 1~3 变换信息组生成各自对应的第 1~7 中间信息组和第 1~3 密码处理信息组。

信息组存贮单元 102 具有信息组更新功能, 每次信息组组合单元 108
20 生成密码文信息组时, 将此密码文信息组作为新链结信息组更新存贮中的链结信息组, 用于处理下一信息组。这里的操作与实施例 7 相同。

信息组组合单元 108, 不是如实施例 7 那样将信息组变换单元 109 生成的变换信息组、而是将第 8 加密单元 105h 生成的密码处理信息组组合到明文信息组生成密码文信息组。在此, 当处理第 1 明文信息组时对 64
25 位的第 1 密码处理信息组与 64 位的第 1 明文信息组进行各对应位的“异或”运算生成 64 位的第 1 密码文信息组, 而当处理第 2~3 明文信息组时对 64 位的第 2~3 密码处理信息组与 64 位的第 2~3 明文信息组进行各对应位的“异或”运算生成 64 位的第 2~3 密码文信息组。

信息组结合单元 107 将信息组组合单元 108 生成的各密码文信息组和
30 尾数数据处理单元 106 生成的尾数密码文数据相结合生成密码文数据。在

此,将各 64 位的第 1~3 密码文信息组和 8 位的尾数密码文数据相结合生成 200 位的密码文数据。

图 37 表示本发明实施例 8 中图 2 所示数据译码装置 20 的详细构成。

此数据译码装置 20 由信息组分割单元 201、信息组存贮单元 202、部分
5 分密钥生成单元 204、第 1~8 加密单元 205i~205p、尾数数据处理单元 206、信息组结合单元 207、信息组组合单元 208 和信息组变换单元 209 构成。

信息组存贮单元 202 具有信息组更新功能,每次信息组分割单元 201 生成密码文信息组时,将此密码文信息组作为新链结信息组更新存贮中的
10 链结信息组,用于下一信息组的处理。在此,预先存贮 64 位的初始值 IV,此初始值 IV 被用于处理第 1 密码文信息组,将第 1 密码文信息组更新作为新的链结信息组。接着,第 1 密码文信息组处理时更新的链结信息组用于处理第 2 密码文信息组,并将第 2 密码文信息组更新为新的链结信息组。然后,第 2 密码文信息组处理时更新的链结信息组在处理第 3 密码文
15 信息组时加以应用,将第 3 密码文信息组更新为新链结信息组。最后,将第 3 密码文信息组处理时更新的链结信息组用于处理尾数密码文数据。

与实施例 8 中图 36 所示数据加密装置 10 同一名称的构成部分具有同样的功能,只有信息组存贮单元 202 的输入与数据加密装置 10 的信息组存贮单元 102 的输入不同,除这一点外,均与数据加密装置 10 相同。

20 图 38 表示本发明实施例 8 的数据加密装置 10 中的加密处理流程。

与实施例 7 中图 34 所示数据加密装置 10 的操作共同的步骤加以同一标号,其说明省略。

(1)~(3)与实施例 7 相同(步骤 S101、S102、S301:第 1 次)。

(4)信息组变换单元 109 对信息组存贮单元 102 中存贮的链结信息
25 组进行预先确定的规定变换生成变换信息组,第 1 加密单元 105a 根据第 1 部分密钥由该变换信息组生成第 1 中间信息组(步骤 S1501)。这里,由 64 位的链结信息组的初始值 IV 生成 64 位的第 1 变换信息组,由此 64 位的第 1 变换信息组生成第 1 中间信息组(步骤 S1501:第 1 次)。

(5)~(6)与实施例 7 的(6)~(7)相同(步骤 S106、S108:
30 第 1 次)。

(7) 第 8 加密单元 105h 根据第 8 部分密钥, 由第 7 中间信息组生成密码处理信息组 (步骤 S1502)。在此, 由对应于链结信息组的初始值 IV 的第 7 中间信息组生成第 1 密码处理信息组 (步骤 S1502: 第 1 次)。

(8) 信息组组合单元 108 将密码处理信息组组合到明文信息组生成
5 密码文信息组 (步骤 S1503)。在此, 对 64 位的第 1 密码处理信息组与 64 位的第 1 明文信息组进行各对应位的“异或”运算, 生成 64 位的第 1 密码文信息组 (步骤 S1503: 第 1 次)。

(9) ~ (13) 与实施例 7 相同 (步骤 S1302、S110: 第 1 次, 步骤 S101、S102、S301: 第 2 次)。

10 (14) 在步骤 S1501, 这里由第 1 明文信息组处理时生成的 64 位的链结信息组生成 64 位的第 2 变换信息组, 由 64 位的第 2 变换信息组生成第 1 中间信息组 (步骤 S1501: 第 2 次)。

(15) ~ (16) 与实施例 7 的 (16) ~ (17) 相同 (步骤 S106、S108: 第 2 次)。

15 (17) 在步骤 S1502, 这里由对应于第 1 明文信息组处理时生成的链结信息组的第 7 中间信息组生成第 2 密码处理信息组 (步骤 S1502: 第 2 次)。

(18) 步骤 S1503 中, 在此对 64 位的第 2 密码处理信息组与 64 位的第 2 明文信息组进行各对应位的“异或”运算, 生成 64 位的第 2 密码文
20 信息组 (步骤 S1503: 第 2 次)。

(19) ~ (23) 与实施例 7 相同 (步骤 S1302、S110: 第 2 次, S101、S102、S301: 第 3 次)。

(24) 步骤 S1501 中, 在此, 由第 2 明文信息组处理时所生成的 64 位的链结信息组生成 64 位的第 3 变换信息组, 由 64 位的第 3 变换信息组
25 生成第 1 中间信息组 (步骤 S1501: 第 3 次)。

(25) ~ (26) 与实施例 7 的 (26) ~ (27) 相同 (步骤 S106、S108: 第 3 次)。

(27) 在步骤 S1502, 这里, 由对应于第 2 明文信息组处理时所生成的链结信息组的第 7 中间信息组生成第 3 密码处理信息组 (步骤 S1502:
30 第 3 次)。

(28) 在步骤 S1503, 这里对 64 位的第 3 密码处理信息组与 64 位的第 3 明文信息组进行各对应位的“异或”运算, 生成 64 位的第 3 密码文信息组(步骤 S1503: 第 3 次)。

(29) ~ (34) 与实施例 7 相同(步骤 S1302、S110: 第 3 次, 步骤 5 S101: 第 4 次, 第 S111~S113)。

数据译码装置 20 的操作为数据加密装置 10 的操作的逆变换。

实施例 8 中数据译码装置 20 的操作, 除信息组存贮单元的输入不同外均与实施例 8 中数据加密装置 10 的操作相同, 其说明省略。

实施例 8 的密码处理装置, 将前面的密码文信息组作为链结信息组存 10 贮, 在后面的密码处理时执行信息组变换和密码处理组合进明文信息组和密码文信息组, 每次进行密码处理时更新该链结信息组。

上述实施例 8 中虽以密码文信息组作为新的链结信息组, 但也可以将明文信息组或任一中间信息组作为新的链结信息组。

<实施例 9>

15 本发明实施例 9 仅信息组存贮单元的输入与实施例 8 不同。

密码通信系统的构成与实施例 1 同样故省略其说明。

图 39 表示本发明实施例 9 中图 2 所示数据加密装置 10 的详细结构。

与实施例 8 中图 36 所示数据加密装置 10 共同的构成部分加以同一标号, 具有同样功能的构成部分的说明省略。

20 此数据加密装置 10 的结构与实施例 8 的结构相同。

信息组存贮单元 102 具有信息组更新功能, 每次第 8 加密单元 105h 生成密码处理信息组时将此密码处理信息组作为新链结信息组更新存贮中的链结信息组, 用于下一信息组的处理。在此, 预先存贮 64 位的初始值 IV, 此初始值 IV 用于处理第 1 明文信息组, 将这一处理时所生成的第 25 1 密码处理信息更新为新的链结信息组。接着, 第 1 明文信息组处理时更新的链结信息组在处理第 2 明文信息组时应用, 将此处理时生成的第 2 密码处理信息组更新为新链结信息组。然后, 第 2 明文信息组处理时更新的链结信息组用于处理第 3 明文信息组, 而将此处理时所生成的第 3 密码处理信息组更新为新链结信息组。最后, 第 3 明文信息组处理时更新的链 30 结信息组用于处理尾数明文数据。

图 40 表示本发明实施例 9 中图 2 所示数据译码装置 20 的详细构成。

此数据译码装置 20 的构成与实施例 8 的构成同样，而且与实施例 9 中图 39 所示数据加密装置 10 同一名称的构成部分具有相同功能，所以其说明省略。

- 5 本发明实施例 9 的数据加密装置 10，除信息组存贮单元 102 的输入不同外，均与实施例 8 的数据加密装置 10 相同，故省略对其操作的说明。

数据译码装置 20 的操作为数据加密装置 10 的操作的逆变换。

实施例 9 中的数据译码装置 20 的操作与实施例 9 中数据加密装置 10 的操作同样，所以其说明省略。

- 10 实施例 9 的密码处理装置，将对前面信息组进行密码处理过程中所生成的密码处理信息组作为新的链结信息组存贮，在后面的密码处理时进行信息组变换和密码处理组合进明文信息组和密码文信息组，每次进行密码处理时更新该链结信息组。

<实施例 10>

- 15 本发明实施例 10 为对实施例 1，在每次处理 1 信息组时另外增加更新关键数据的功能。

密码通信系统的构成与实施例 1 相同，其说明省略。

图 41 表示本发明实施例 10 中图 2 所示数据加密装置 10 的详细构成。

- 20 与实施例 1 中图 3 所示数据加密装置 10 共同的构成部分加以同一标号，具有相同功能的结构部分的说明省略。

此数据加密装置 10 由信息组分割单元 101、信息组存贮单元 102、关键数据组合单元 103、部分密钥生成单元 104、第 1~8 加密单元 105a~105h、尾数数据处理单元 106、信息组结合单元 107 和关键数据存贮单元 110 构成。

- 25 图 1 所示的历来的加密装置 30 与图 41 所示本发明实施例 10 中的数据加密装置 10 的关系与实施例 1 相同，另外加有关键数据存贮单元 110。

关键数据存贮单元 110 存贮关键数据，在处理最初的信息组时预先存贮关键数据的初始值。

- 30 关键数据组合单元 103 将信息组存贮单元 102 中存贮的链结信息组合进关键数据存贮单元 110 中存贮的关键数据，生成组合关键数据。这

里, 在处理第 1 明文信息组时, 对 64 位的链结信息组的初始值 IV 与 64 位的键数据初始值进行各对应位的“异或”运算, 在处理第 2~3 明文信息组时, 对第 1~2 明文信息组处理时所生成的 64 位的链结信息组与第 1~2 明文信息组处理时所生成的 64 位的键数据进行各对应位的“异或”运算。

关键数据存贮单元 110 有关键数据更新功能, 每次关键数据组合单元 103 生成组合关键数据时, 即将组合关键数据作为新的关键数据更新存贮中的关键数据, 用于下一信息组处理。在这里, 预先存贮 64 位的初始值, 将此初始值用于处理第 1 明文信息组, 将此处理时所生成的组合关键数据更新为新的关键数据。接着, 第 1 明文信息组处理时更新的关键数据用于处理第 2 明文信息组, 将此处理时所生成的组合关键数据更新为新的关键数据。然后, 第 2 明文信息组处理时更新的关键数据在处理第 3 明文信息组时加以利用, 将此处理时所生成的组合关键数据更新为新的关键数据。

图 42 表示本发明实施例 10 中图 2 所示数据译码装置 20 的详细构成。与实施例 1 中图 8 所示数据译码装置 20 共同的构成部分加以同一标号, 具有相同功能的构成部分的说明省略。

此数据译码装置 20 由信息组分割单元 201、信息组存贮单元 202、关键数据组合单元 203、部分密钥生成单元 204、第 1~8 译码单元 205a~205h、尾数数据处理单元 206、信息组结合单元 207 和关键数据存贮单元 210 构成。

关键数据存贮单元 210 存贮关键数据。而在处理最初的信息组时预先存贮关键数据的初始值。

关键数据组合单元 203 将信息组存贮单元 202 中所存贮的链结信息组组合进关键数据存贮单元 210 中存贮的关键数据, 生成组合关键数据。这里, 在处理第 1 密码文信息组时, 对 64 位的链结信息组的初始值 IV 与 64 位的键数据初始值进行各对应位的“异或”运算生成第 1 组合关键数据, 而在处理第 2~3 密码文信息组时, 对第 1~2 密码文信息组处理时分别生成的 64 位的链结信息组与第 1~2 密码文信息组处理时分别生成的 64 位的键数据进行各对应位的“异或”运算生成第 2~3 组合关键数据。

关键数据存贮单元 210 具有关键数据更新功能, 每次关键数据组合单

元 203 生成组合关键数据时,将组合关键数据作为新的关键数据更新存贮着的
5 关键数据,用于下一信息组的处理。在此,预先存贮 64 位的初始值,将此初始值用于处理第 1 密码文信息组,将此处理时所生成的第 1 组合关键数据更新为新关键数据。接着,将第 1 密码文信息组处理时更新的关键数据用于处理第 2 密码文信息组,并将此处理时生成的第 2 组合关键数据更新为新关键数据。然后,第 2 密码文信息组处理时更新的关键数据在处理第 3 密码文信息组对应用,将此处理时所生成的第 3 组合关键数据更新为新关键数据。

图 43 表示本发明实施例 10 的数据加密装置 10 中的加密处理流程。

10 与实施例 1 中图 10 所示数据加密装置 10 的操作共同的步骤加以同一标号,其说明省略。

这里,对实施例 1 的条件,还在关键数据存贮单元 110 中预先存贮关键数据的初始值。

(1) ~ (2) 与实施例 1 同样(步骤 S101、S102: 第 1 次)。

15 (3) 关键数据组合单元 103 将信息组存贮单元 102 中存贮的链结信息组组合到关键数据存贮单元 110 中存贮的关键数据生成组合关键数据,关键数据存贮单元 110 将此组合关键数据作为新关键数据更新自身存贮的关键数据(步骤 S1601)。在此,对信息组存贮单元 102 中存贮的 64 位的初始值 IV 与关键数据存贮单元 110 中存贮的 64 位的关键数据的初始
20 值进行各对应位的“异或”运算,生成第 1 组合关键数据传送给部分密钥生成单元 104,将此第 1 组合关键数据作为新关键数据更新关键数据(步骤 S1601: 第 1 次)。

(4) ~ (12) 与实施例 1 相同(步骤 S104~S110: 第 1 次, S101、S102: 第 2 次)。

25 (13) 在步骤 S1601, 这里对第 1 明文信息组处理时所生成的 64 位的链结信息组与第 1 明文信息组处理时生成的 64 位的关键数据进行各对应位的“异或”运算,生成第 2 组合关键数据传送到部分密钥生成单元 104,将第 2 组合关键数据作为新关键数据更新关键数据(步骤 S1601: 第 2 次)。

30 (14) ~ (22) 与实施例 1 相同(步骤 S104~110: 第 2 次, S101、

S102: 第3次)。

(23) 在步骤 S1601, 这里, 对第2明文信息组处理时所生成的64位的链结信息组与第2明文信息组处理时所生成的64位的关键数据进行各对应位的“异或”运算, 生成第3组合链数据传送到部分密钥生成单元
5 104, 将此第3组合关键数据作为新关键数据更新关键数据(步骤 S1601: 第3次)。

(24) ~ (34) 与实施例1相同(步骤 S104~S110: 第3次, 步骤 S101: 第4次, S111~S113)。

图44表示本发明实施例10的数据译码装置20中的加密处理流程。
10 数据译码装置20的操作为数据加密装置10的操作的逆变换。

与实施例1中图11所示数据译码装置20的操作共同的步骤加以同一标号, 其说明省略。

(1) ~ (2) 与实施例1相同(步骤 S201、S202: 第1次)。

(3) 关键数据组合单元203将信息组存贮单元202中存贮的链结信息
15 息组组合到关键数据存贮单元210中存贮的关键数据生成组合关键数据, 关键数据存贮单元210将此组合关键数据作为新的关键数据更新自身存贮的关键数据(步骤 S1701)。在此, 对信息组存贮单元202中存贮的64位的初始值IV与关键数据存贮单元210存贮的64位的关键数据的初始值进行各对应位的“异或”运算, 生成第1组合关键数据传送到部分密
20 钥生成单元204, 将第1组合关键数据作为新关键数据更新关键数据(步骤 S1701: 第1次)。

(4) ~ (12) 与实施例1相同(步骤 S204S210: 第1次, S201、S202: 第2次)。

(13) 在步骤 S1701, 这里, 对第1密码文信息组处理时生成的64
25 位的链结信息组与第1密码文信息组处理时生成的64位的关键数据进行各对应位的“异或”运算, 生成第2组合关键数据传送到部分密钥生成单元204, 将第二组合关键数据作为新关键数据更新关键数据(步骤 S1701: 第2次)。

(14) ~ (22) 与实施例1相同(步骤 S204~S210: 第2次, S201、
30 S202: 第3次)。

(23) 在步骤 S1701, 这里, 对第 2 密码文信息组处理时生成的 64 位的链结信息组与第 2 密码文信息组处理时生成的 64 位的关键数据进行各对应位的“异或”运算, 生成第 3 组合关键数据传送到部分密钥生成单元 204, 将第 3 组合关键数据作为新关键数据更新关键数据。

5 <步骤 S1703: 第 3 次>。

(24)~(34) 与实施例 1 相同, (步骤 S204~S210: 第 3 次, S201: 第 4 次, S211~S213)。

实施例 10 的密码处理装置, 将对前面信息组进行密码处理的过程中所生成的中间信息组和组合关键信息组作为链结信息组和关键信息组存
10 贮, 在后面的密码处理时将链结信息组组合到关键信息组, 在每次执行密码处理时更新该链结信息组和关键信息组。

虽然是上述实施例 10 中, 在实施例 1 的数据加密装置 10 上增加关键数据存贮单元 110, 在实施例 1 的数据译码装置 20 上增加关键数据存贮单元 210, 但也可对其他实施例 2~9 同样地增加关键数据存贮单元 110
15 和关键数据存贮单元 210。

<实施例 11>

本发明实施例 11 为对实施例 1 另外还增加根据存贮的链结信息组由输出信息组、被作密码处理信息组和中间信息组等中选取 1 个信息组的功能。

20 密码通信系统的构成与实施例 1 相同, 其说明省略。

图 45 表示本发明实施例 11 中图 2 所示数据加密装置 10 的详细构成。

与实施例 1 中的图 3 所示数据加密 10 共同的构成部分加以同一标号, 具有同一功能的构成部分的说明省略。

此数据加密装置 10 由信息组分割单元 101、信息组存贮单元 102、关键数据组合单元 103、部分密钥生成单元 104、第 1~8 加密单元 105a~
25 105h、尾数数据处理单元 106、信息组结合单元 107 和信息组选择单元 111 构成。

图 1 所示的历来的加密装置 30 与图 45 所示本发明实施例 11 中的数据加密装置 10 的关系与实施例 1 同样, 另外附加有信息组选择单元 111。

30 信息组选择单元 111 根据信息组存贮单元 102 中存贮的链结信息组,

由明文信息组、各中间信息组和密码文信息组中选择 1 个信息组，传送到信息组存贮单元 102。具体说，例如，在信息组存贮单元 102 中存贮的链结信息组的低 3 位为“001”时选择第 1 中间信息组，同样地，在“010”～“111”的情况下选择第 2 中间信息组～第 7 中间信息组。而在链结信息组的低 3 位为“000”的情况下，当低位第 4 位为“0”时选择明文信息组，低位第 4 位为“1”时选择密码文信息组。

信息组存贮单元 102 将信息组选择单元 111 所选择的信息组作为新的链结信息组更新存贮中的链结信息组，在处理下一信息组时利用。这里，预先存贮 64 位的初始值 IV，此初始值 IV 被用于处理第 1 明文信息组，将根据此初始值 IV 的低 4 位选择的信息组更新作为新的链结信息组。接着，第 1 明文信息组处理时更新的链结信息组在处理第 2 明文信息组时应用，将根据此链结信息组的低 4 位选择的信息组更新为新链结信息组。然后，第 2 明文信息组处理时更新的链结信息组被用于处理第 3 明文信息组，将根据此链结信息组的低 4 位选择的信息组更新为新的链结信息组。最后，第 3 明文信息组处理时更新的链结信息组被用于处理尾数明文数据。

图 46 表示本发明实施例 11 中图 2 所示数据译码装置 20 的详细构成。

与实施例 1 中图 8 所示数据译码装置 20 共同的构成部分加以同一标号，具有相同功能的构成部分的说明省略。

此数据译码装置 20 由信息组分割单元 201、信息组存贮单元 202、关键数据组合单元 203、部分密钥生成单元 204、第 1～8 译码单元 205a～205h、尾数数据处理单元 206、信息组结合单元 207 和信息组选择单元 211 构成。

信息组选择单元 211 根据信息组存贮单元 202 中存贮的链结信息组，由密码文信息组、各中间信息组和明文信息组中选择 1 个信息组，传送到信息组存贮单元 202。具体地说，例如，在信息组存贮单元 202 中存贮的链结信息组的低 3 位的“001”时选择第 1 中间信息组，同样地，在“010”～“111”时选择第 2 中间信息组～第 7 中间信息组。而在链结信息组的低 3 位为“000”的情况下，低位第 4 位为“0”时选择明文信息组，低位第 4 位为“1”时选择密码文信息组。

信息组存贮单元202将信息组选择单元211选择的信息组作为新链结信息组更新存贮中的链结信息组，用于处理下一信息组。在此，预先存贮64位的初始值IV，此初始值IV用于处理第1密码文信息组，将根据此初始值IV的低4位选择的信息组更新为新链结信息组。接着，将第1密码文信息组处理时更新的链结信息组用于处理第2密码文信息组，将根据此链结信息组低4位选择的信息组更新为新链结信息组。然后，第2密码文信息组处理时更新的链结信息组再用于处理第3密码文信息组，将根据此链结信息组低4位选择的信息组更新为新链结信息组。最后，第3密码文信息组处理时更新的链结信息组用于尾数密码文数据的处理。

10 图47表示本发明实施例11的数据加密装置10中的加密处理流程。

与实施例1中图10所示数据密码文装置10的操作共同的步骤加以同一标号，其说明省略。

(1)～(8)与实施例1的(1)～(6)、(8)、(9)相同(步骤S101～S106、S108、S109：第1次)。

15 (9)信息组选择单元111根据信息组存贮单元102中存贮的链结信息组，由明文信息组、各中间信息组和密码文信息组中选择1个信息组，信息组存贮单元102将所选择的信息组作为新链结信息组更新存贮中的链结信息组(步骤S1801)。在此，例如，如假定信息组存贮单元102中存贮的链结信息组的初始值IV的低3位为“011”，即选择对应于第1
20 明文信息组的第3中间信息组，将所选择的第3中间信息组作为新链结信息组更新链结信息组(步骤S1801：第1次)。

(10)～(18)与实施例1相同(步骤S110：第1次，S101～S106、S108、S109：第2次)。

(19)在步骤S1801，这里，例如，第1明文信息组处理时生成选择的链结信息组的低4位为“0000”，即选择第2明文信息组，将所选择的第2明文信息组作为新链结信息组更新链结信息组(步骤S1801：第2
25 次)。

(20)～(28)与实施例1同样(步骤S110：第2次，S101～S106、S108、S109：第3次)。

30 (29)在步骤S1801中，这里例如第2明文信息组处理时生成选择的

链结信息组的低4位为“1000”，即选择第3密码文信息组，将所选择的第3密码文信息组作为新链结信息组更新链结信息组（步骤S1801：第3次）。

（30）～（34）与实施例1相同（步骤S110：第3次，S101：第4次，S111～S113）。

图48表示本发明实施例11的数据译码装置20中的加密处理流程。

数据译码装置20的操作为数据加密装置10的操作的逆变换。

与实施例1中图11所示数据译码装置20的操作共同的步骤加以同一标号，其说明省略。

（1）～（8）与实施例的（1）～（6）、（8）、（9）相同（步骤S201～S206、S208、S209：第1次）。

（9）信息组选择单元211根据信息组存贮单元202中存贮的链结信息组，由密码文信息组、各中间信息组和明文信息组中选择一个信息组，信息组存贮单元202将所选择的信息组作为新的链结信息组更新存贮中的链结信息组（步骤S1901）。这里，例如，信息组存贮单元202中存贮的链结信息组的初始值IV的低3位为“011”，即选择对应于第1密码文信息组的第3中间信息组，将所选择的第3中间信息组作为新链结信息组更新链结信息组（步骤S1901：第1次）。

（10）～（18）与实施例1同样（步骤S210：第1次，S201～S206、S208、S209：第2次）。

（19）在步骤S1901，这里，例如，第1密码文信息组处理时生成选择的链结信息组的低4位为“0000”，即选择第2明文信息组，将所选择的第2明文信息组作为新链结信息组更新链结信息组（步骤S1901：第2次）。

（20）～（28）与实施例1相同（步骤S210：第2次，S201～S206、S208、S209：第3次）。

（29）在步骤S1901，这里例如，第2密码文信息组处理时生成选择的链结信息组的低4位为“1000”，即选择第3密码文信息组，将所选择的第3密码文信息组作为新链结信息组更新链结信息组（步骤S1901：第3次）。

(30) ~ (34) 与实施例 1 相同 (步骤 S210: 第 3 次, 步骤 S201: 第 4 次, S211~S213)。

实施例 11 的密码处理装置, 将对前面信息信息组进行密码处理的过程中生成的中间信息组等作为链结信息组存贮, 在后面的密码处理时组合
5 进链结数据, 在每次进行密码处理时根据该链结信息组由多个中间信息组等中选择 1 个信息组更新该链结信息组。

上述实施例 11 中, 是在实施例 1 的数据加密装置 10 上加以信息组选择单元 111、在实施例 1 的数据译码装置 20 上加以信息组选择单元 211, 但也可以在其他实施例 2~10 上同样地加以信息组选择单元 111 和信息组
10 选择单元 211。

(实施例 12)

本发明实施例 12 为改变实施例 1 的数据加密装置 10 中尾数数据处理单元 106 进行的尾数数据的处理。

密码通信系统的构成与实施例 1 同样, 说明省略。

15 此数据加密装置 10 的结构与实施例 1 的结构相同。

具有与实施例 1 中图 3 所示数据加密装置 10 同样功能的构成部分的说明省略。

图 49 表示本发明实施例 12 中尾数数据处理单元 106 的详细结构。

尾数数据处理单元 106 在由信息组分割单元 101 接收到尾数明文数据
20 时, 将紧接前面处理的密码文信息组传送给第 1~8 加密单元 105a~105h 使之作加密处理, 根据信息组存贮单元 102 中存贮的链结信息组, 对紧前面处理过的密码文信息组进行密码处理生成尾数数据处理用信息组, 据此, 由尾数明文数据生成与尾数明文数据位数相同的尾数密码文数据, 此单元 106 包含数据匹配单元 106a、尾数数据组合单元 106b 和密码文信息
25 组存贮单元 106c。

密码文信息组存贮单元 106c 存贮在紧接尾数数据处理之前处理过的密码文信息组, 在对尾数数据进行处理时, 将存贮的密码文信息组传送到第 1~8 加密单元 105a~105h。在此, 存贮第 3 密码文信息组, 在对尾数明文信息组进行处理时, 将存贮中的第 3 密码文信息组传送到第 1~8 加
30 密单元 105a~105h。

这里，第1~8加密单元105a~105h，借助执行与实施例1同样的处理，由从密码文信息组存贮单元106c传来的密码文信息组生成尾数数据处理用信息组。在此，由第3密码文信息组生成尾数数据处理用信息组。

数据匹配单元106a由执行密码处理所生成的尾数数据处理用信息组
5 生成与尾数明文数据位数相同的匹配数据。这里，因尾数明文数据为8位，而生成由尾数数据处理用信息组的例如高8位构成的匹配数据。

尾数数据组合单元106b将匹配数据组合到尾数明文数据。这里，对8位的匹配数据与8位的尾数明文数据进行各对应位的“异或”运算，生成8位的尾数密码文数据。

10 此数据加密装置10的操作与图10所示实施例1的加密装置10的操作相同。

图50表示本发明实施例12的数据加密装置10的尾数数据处理流程。

在此作为举例，对取得200位的明文数据，在信息组存贮单元102
15 中预先存贮初始值IV，在第1~3明文信息组的加密已经结束时，将第3密码文信息组存贮进密码文信息组存贮单元106c，剩余的8位作为尾数明文数据由信息组分割单元101向尾数数据处理单元106传送，按DES的算法作为依据加以说明：

（1）关键数据组合单元103，将信息组存贮单元102中存贮的链结
20 信息组组合到关键数据，生成组合关键数据（步骤S2001）。在此，对第3明文信息组处理时所生成的链结信息组与64位的关键数据进行各对应位的“异或”运算，生成组合关键数据传送到部分密钥生成单元104。

（2）部分密钥生成单元104由组合关键数据生成相当于加密单元数的数量的部分密钥（步骤S2002）。这里，由64位的组合关键数据生成8
25 个的48位部分密钥。

（3）第1加密单元105a根据第1部分密钥，由密码文信息组存贮单元106c所存贮的紧前面处理的密码文信息组生成第1中间信息组（步骤S2003）。在此，由第3密码文信息组生成第1中间信息组。

（4）第2~7加密单元105b~105g分别根据第2~7部分密钥由第1~
30 6中间信息组生成第2~7中间信息组（步骤S2004）。在此，由对应于第

3 密码文信息组的第 1~6 中间信息组生成第 2~7 中间信息组。

(5)第 8 加密单元 105h 根据第 8 部分密钥由第 7 中间信息组生成尾数数据处理用信息组(步骤 S2005)。这里,由对应于第 3 密码文信息组的第 7 中间信息组生成尾数数据处理用信息组。

5 (6)数据匹配单元 106a 由执行密码处理所生成的尾数数据处理用信息组生成与尾数明文数据相同位数的匹配数据(步骤 S2006)。这里因尾数明文数据为 8 位,故生成由尾数数据处理用信息组的例如高 8 位构成的匹配数据。

10 (7)尾数数据组合单元 106b 将匹配数据组合进尾数明文数据(步骤 S2007)。在此,对 8 位的匹配数据与 8 位的尾数明文数据进行各对应位的“异或”运算,生成 8 位的尾数密码文数据。

(8)信息组结合单元 107 将第 8 加密单元 105h 生成的各密码文信息组与尾数数据处理单元 106 生成的尾数密码文数据相结合生成密码文数据(步骤 S2008)。这里,将分别对应于第 1~3 明文信息组的各密码文
15 信息组与尾数密码文数据相结合生成 200 位的密码文数据。

数据加密装置 10 中尾数数据处理单元 106 进行的尾数数据的处理没有变更,而数据译码装置 20 中尾数数据处理单元 206 进行的尾数数据的处理也要变化。其变化内容是,根据链结信息组依靠将前面的密码文信息组作为新的输入信息组进行密码文处理生成尾数数据处理用信息组,据此
20 由尾数明文数据生成与尾数明文数据相同位数的尾数密码文数据,因为是与尾数数据处理单元 106 相同的变更,所以省略其说明。

在上述实施例 12 中,虽是变更实施例 1 的尾数数据处理单元 106 进行的尾数数据的处理和尾数数据处理单元 206 进行的尾数数据的处理,但也可在其他实施例 2~11 中同样地改变尾数数据的处理。

25 原来的 DES 算法是要在由各密码处理单元进行加密处理之前进行初始转置,在经 16 级加密处理之后进行最后转置,为了上述各实施例中说明的简单化起见,省略了初始转置、最后转置和 9 段以后的密码处理单元。

上述各实施例的算法并不限于 DES 的算法,怎样的算法均可。因而
30 更不用说,密码处理单元的级数也不限于 8 级,任何级均可。

在上述实施例中，虽主要以第4级的输出作为新的链结信息组，不言而喻，这并不限于第4级，哪一级的输出均可。

上述各实施例中是对链结信息组与关键数据的位数相同的情况加以说明，但它们不一定相同也可以。在将链结信息组等与关键数据组合的各
5 实施例中，在链结信息组与关键数据的位数不同的情况下，由应组合到关键数据的信息组生成与关键数据相同位数的数据，将其组合到关键数据。例如这里，在关键数据的位数大于64位时，依靠对应组合到关键数据的信息组作扩大转置等生成与关键数据相同位数的数据，而在关键数据的位数小于64位时，则生成由关键数据的位数大小的高位来构成的数据，将
10 其组合到关键数据。

上述各实施例中是由数据加密装置10输入明文数据进行加密，而由数据译码装置20对密码文数据进行译码，但因为数据加密装置10中的加密与数据译码装置20中的译码存在着逆变换的关系，所以各自既可成为加密装置也可成为译码装置。因此在上述各实施例中也可以是上述各数据
15 解密装置20输入明文数据进行加密，而上述各数据加密装置10对密码文数据进行译码。

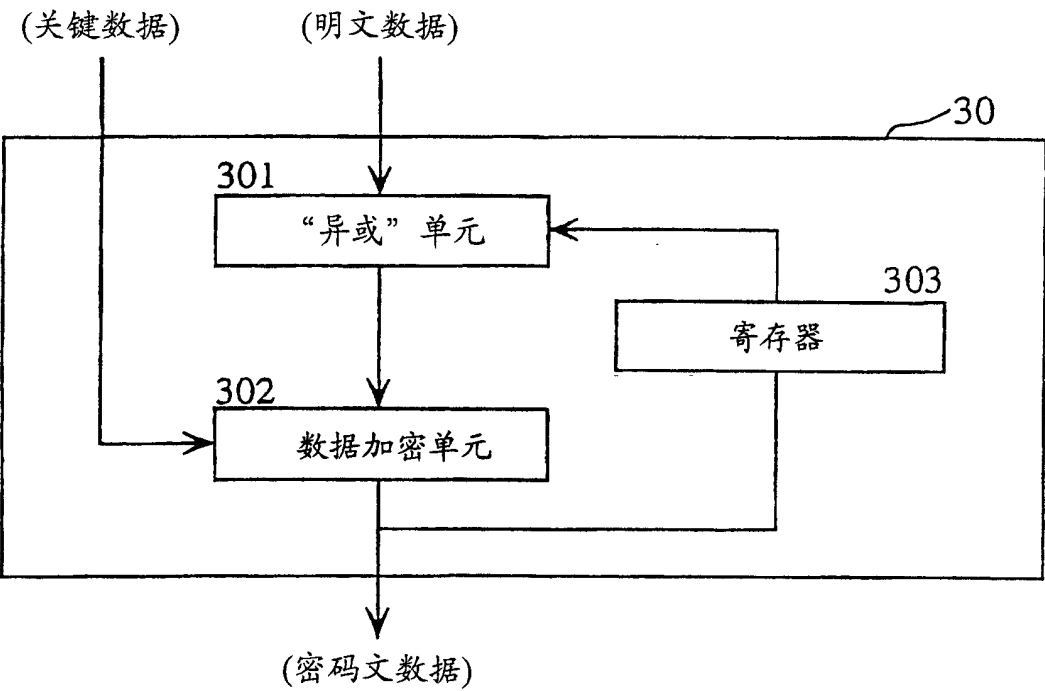


图 1

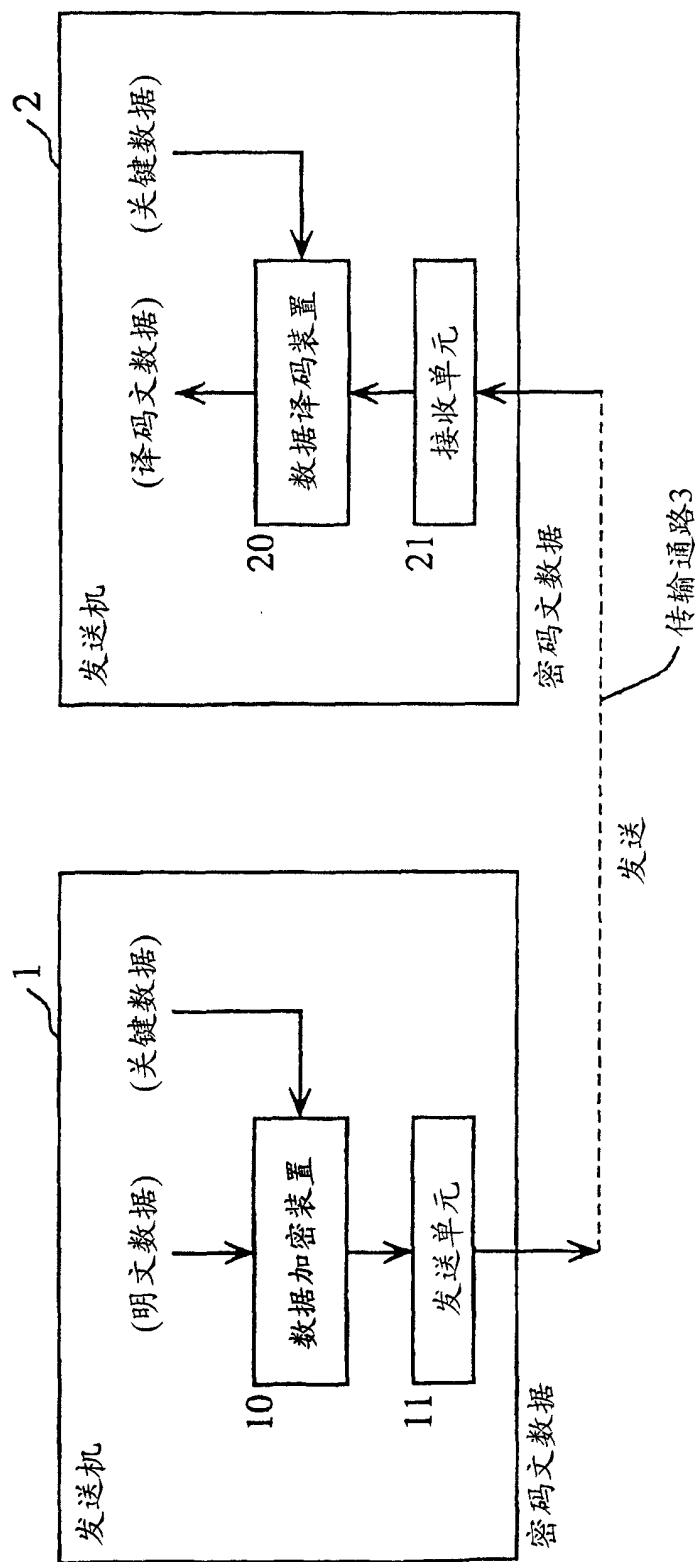


图 2

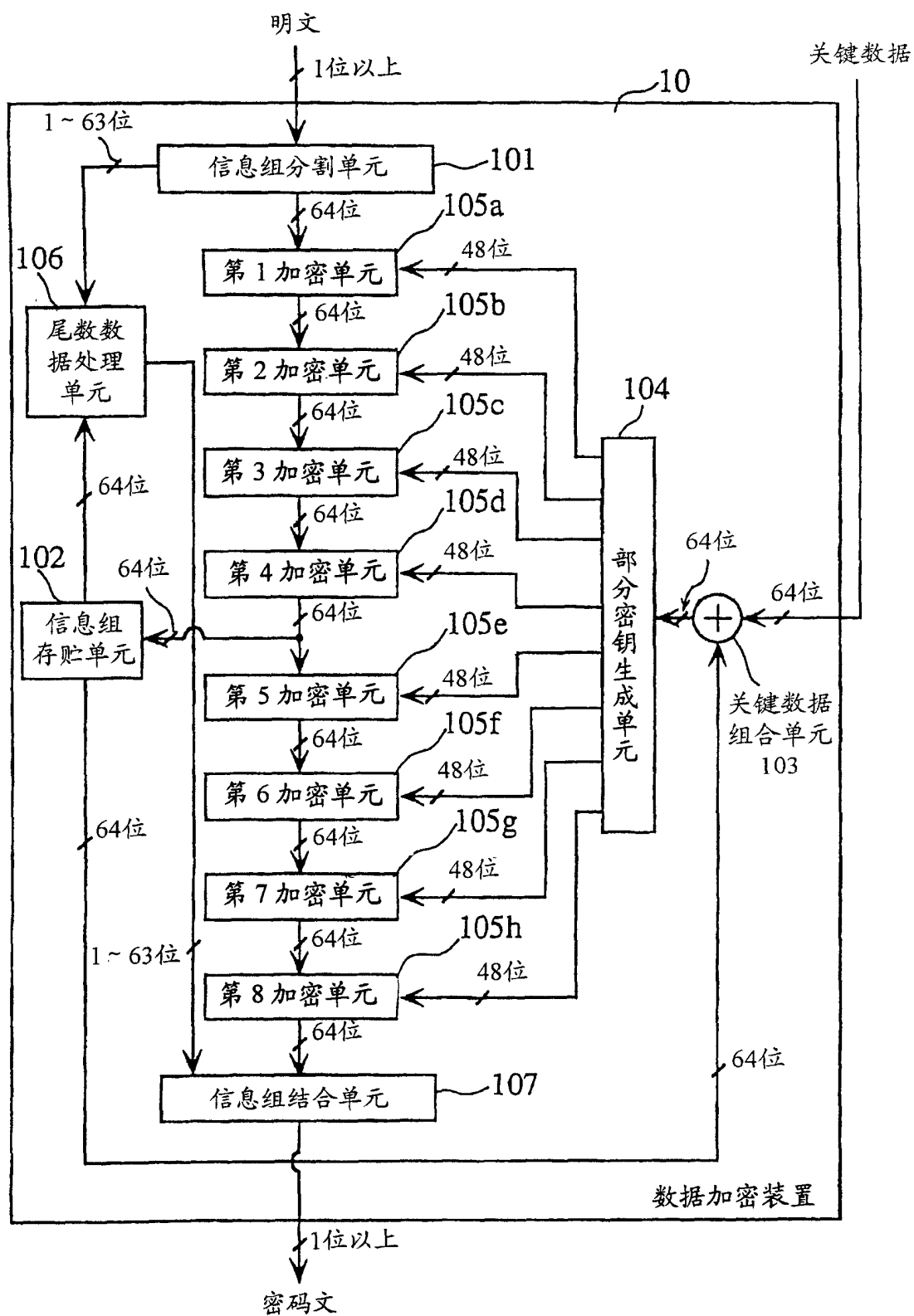


图 3

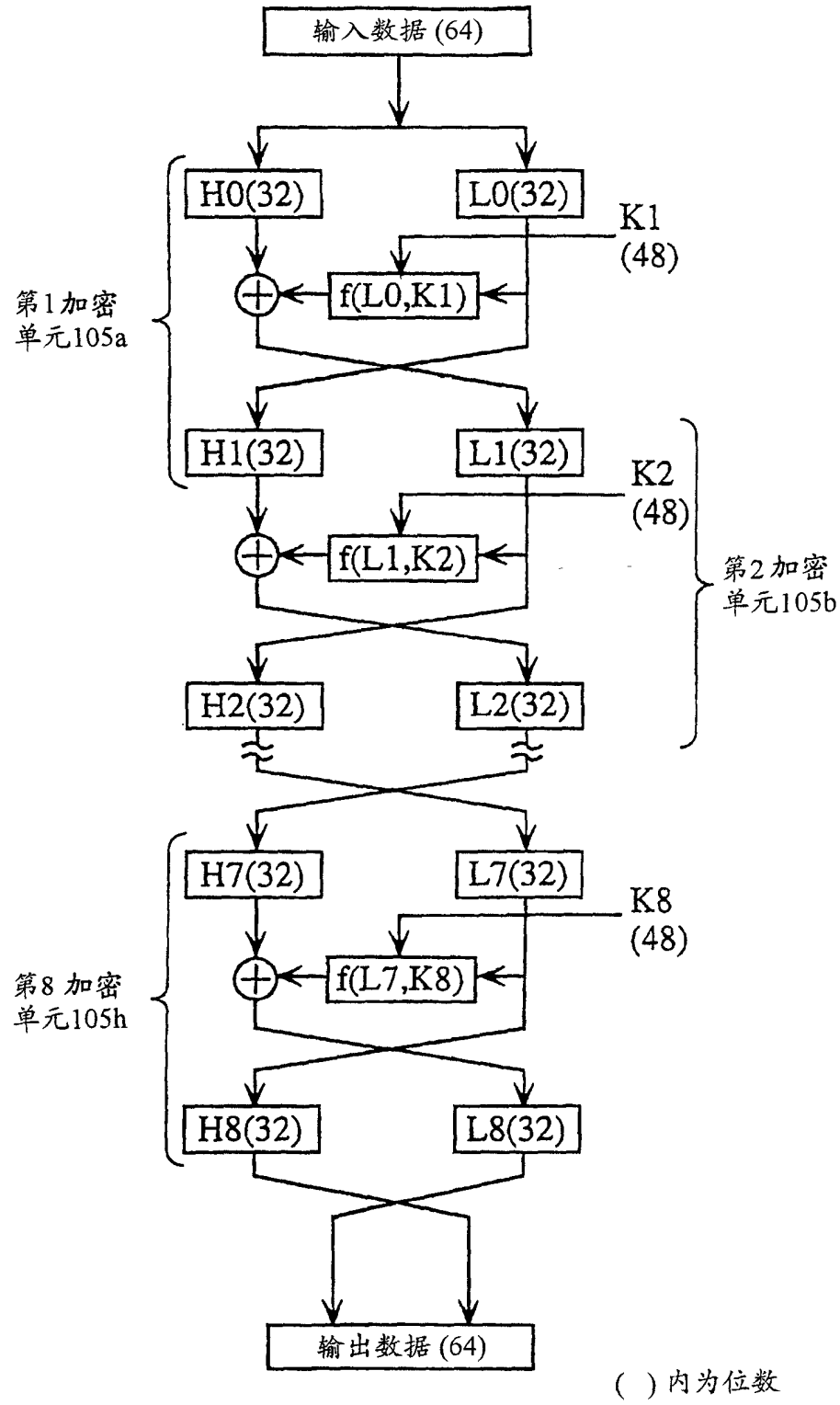


图 4

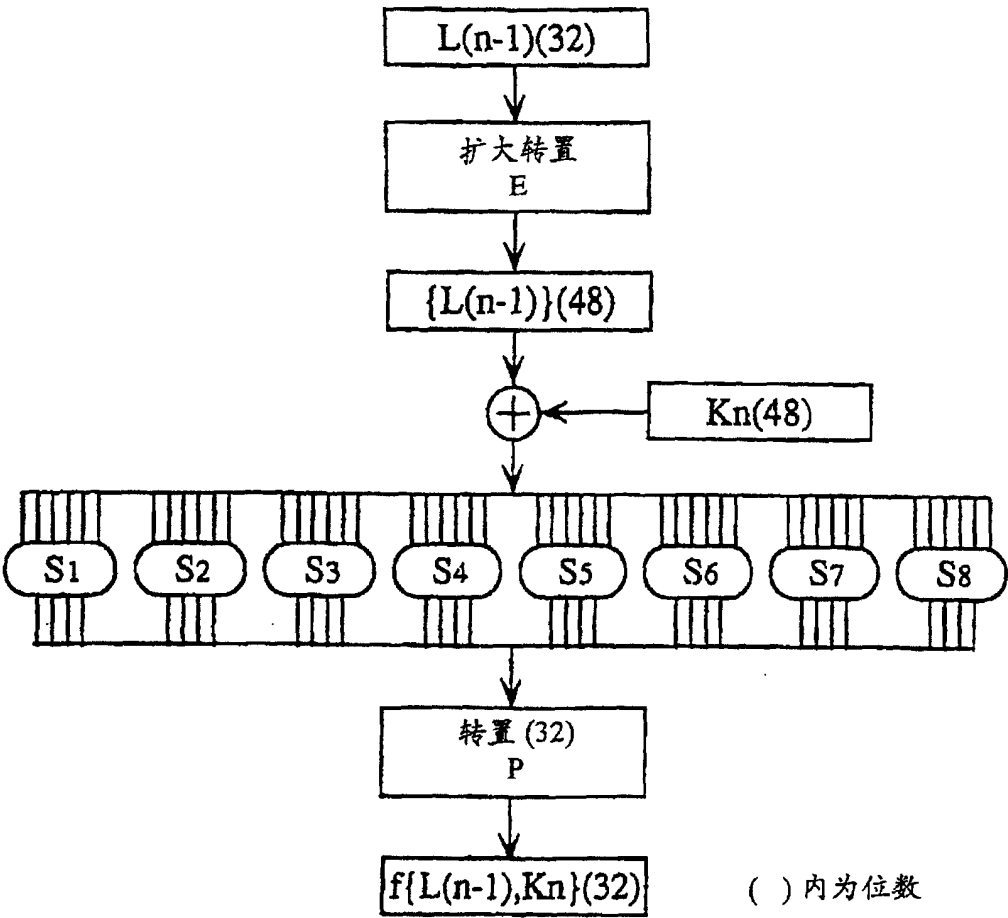
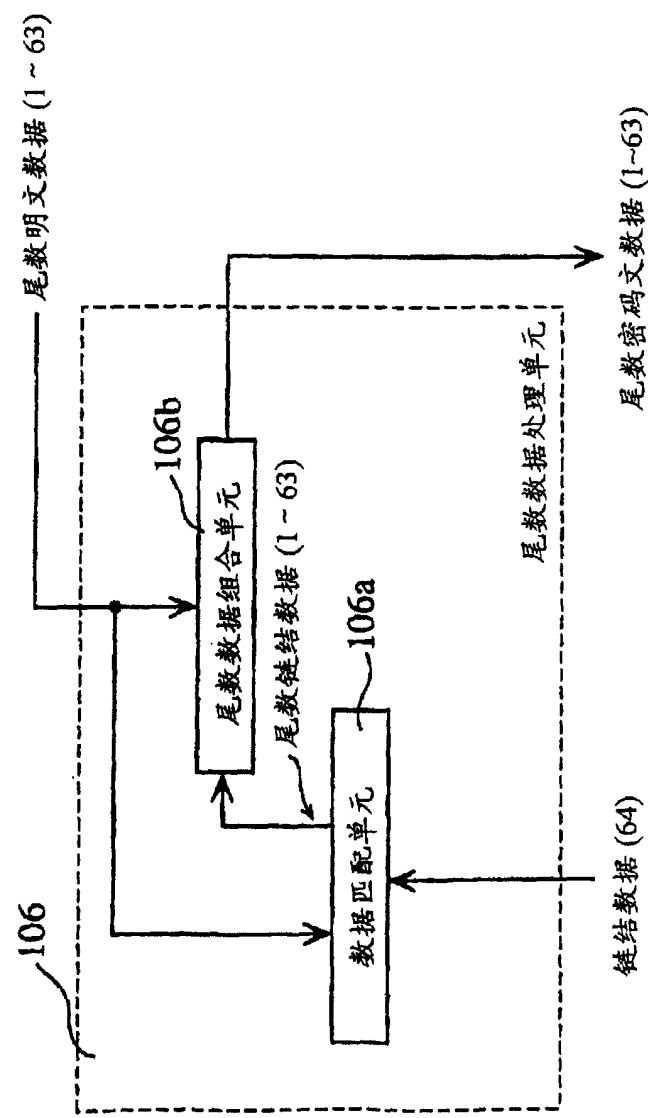


图 5

S ₁															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S ₂															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S ₃															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S ₄															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S ₅															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S ₆															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S ₇															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S ₈															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

图 6



() 为位数

图 7

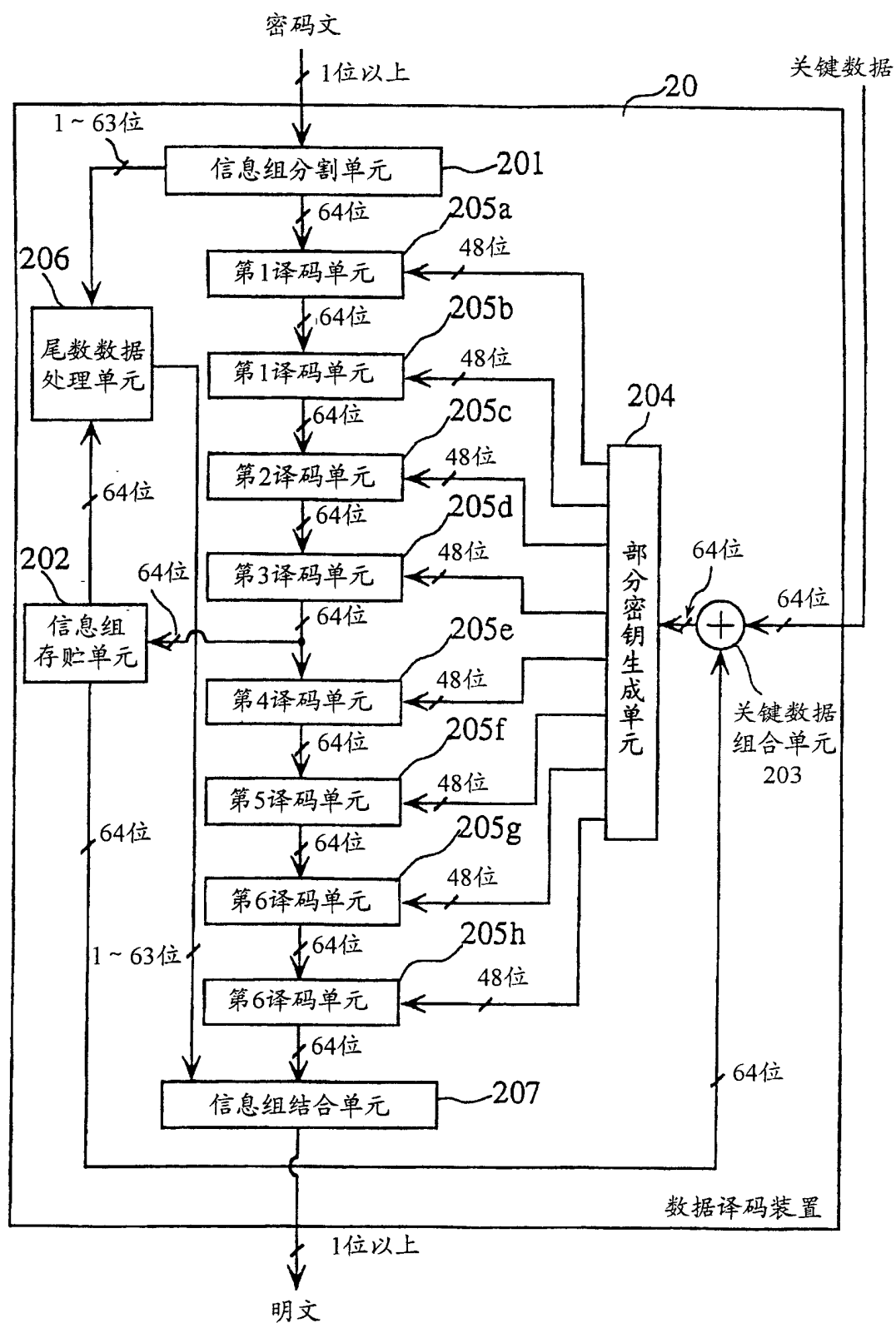


图 8

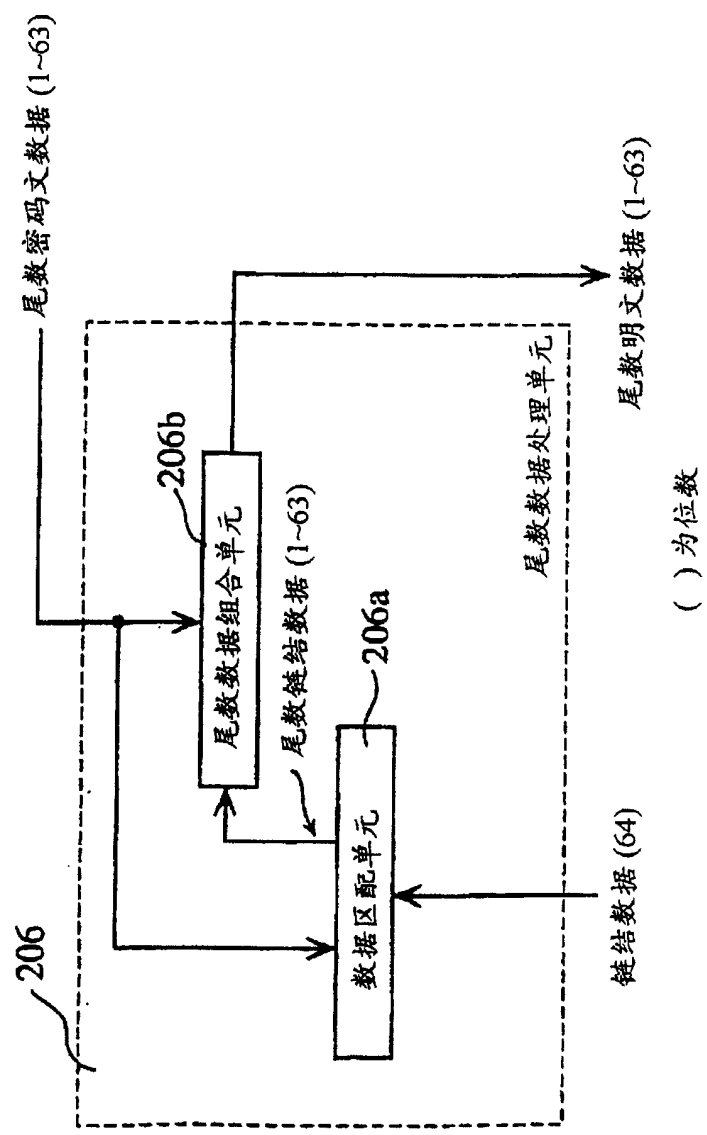


图 9

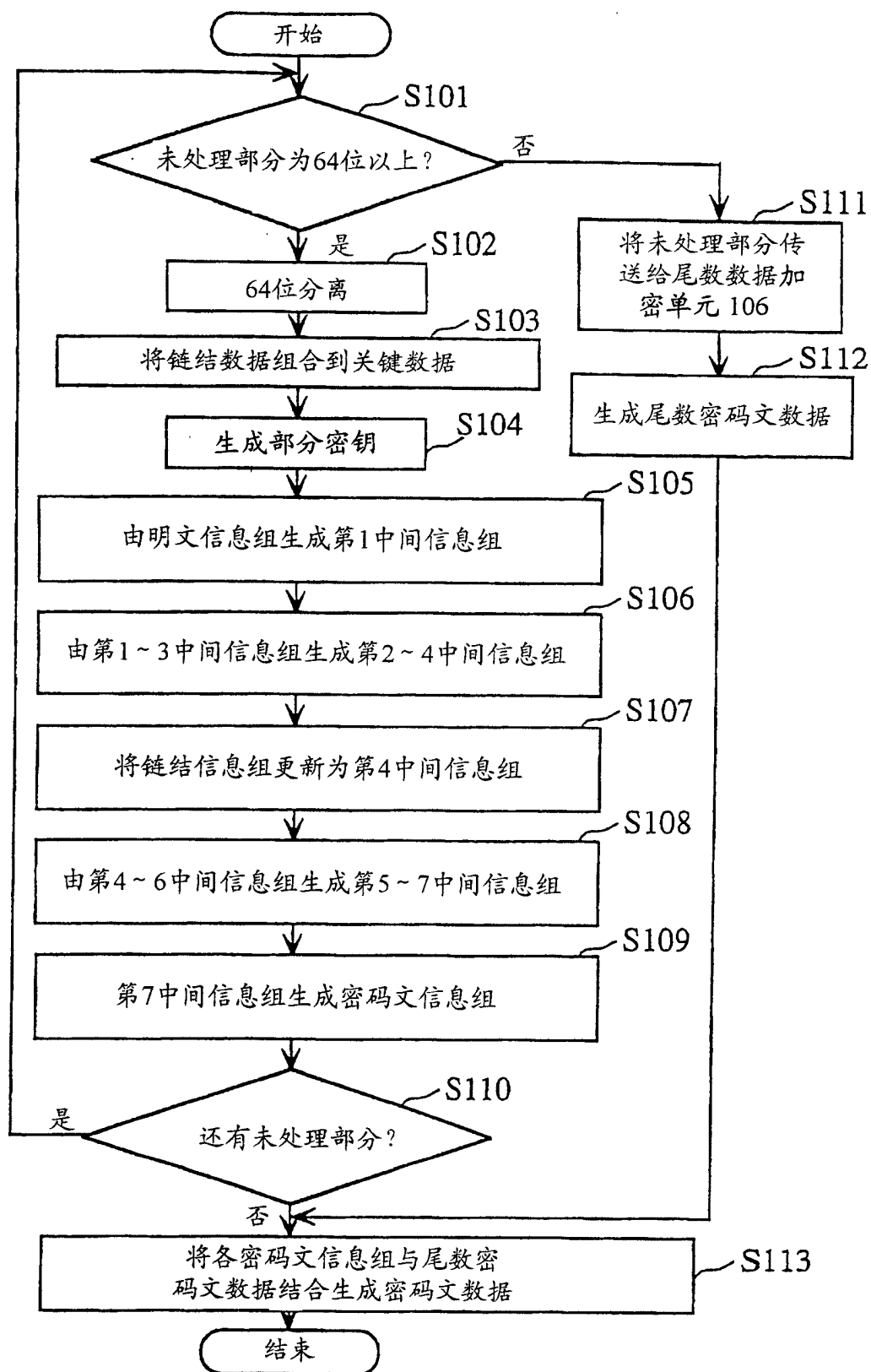


图 10

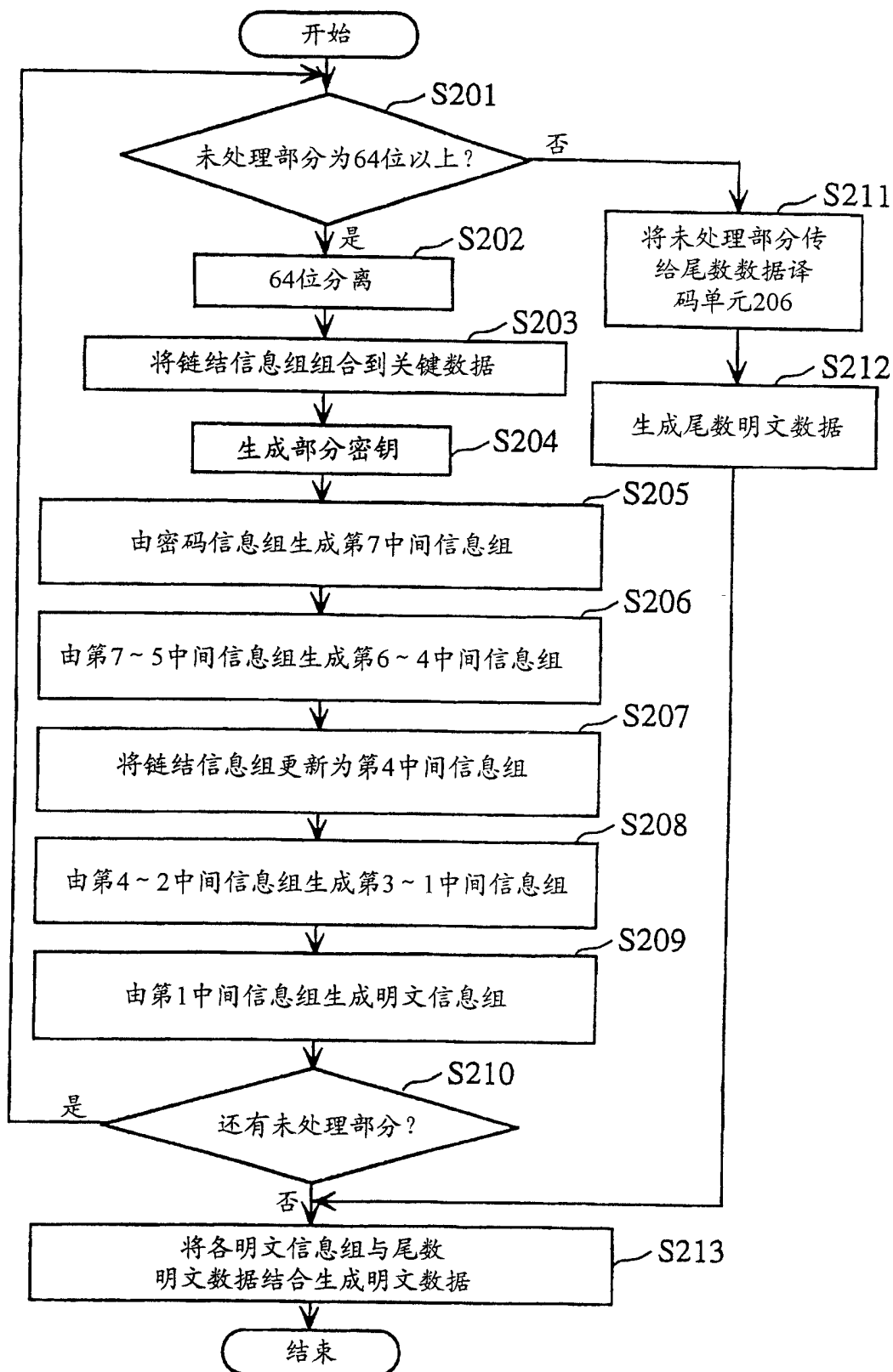


图 11

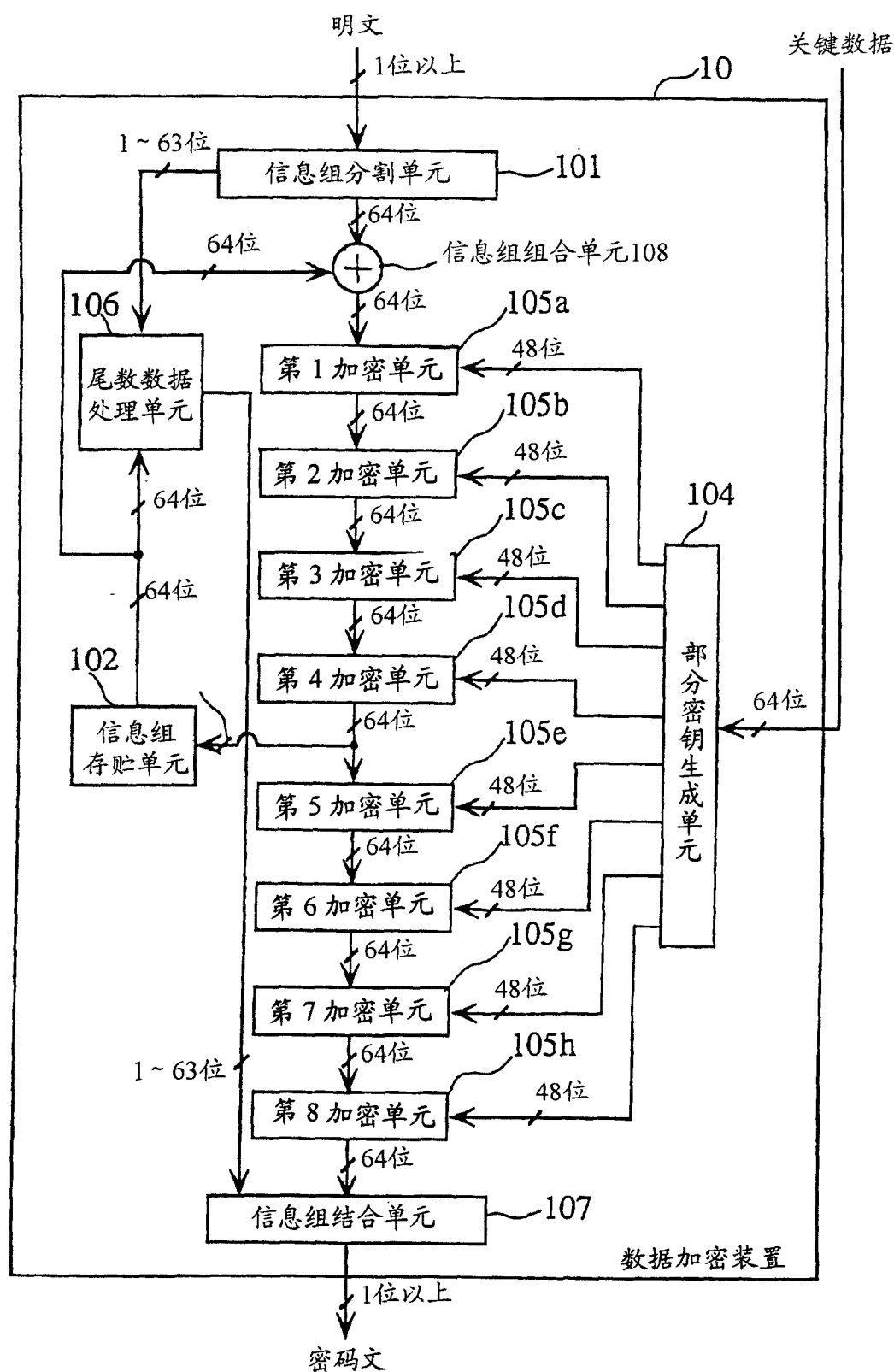


图 12

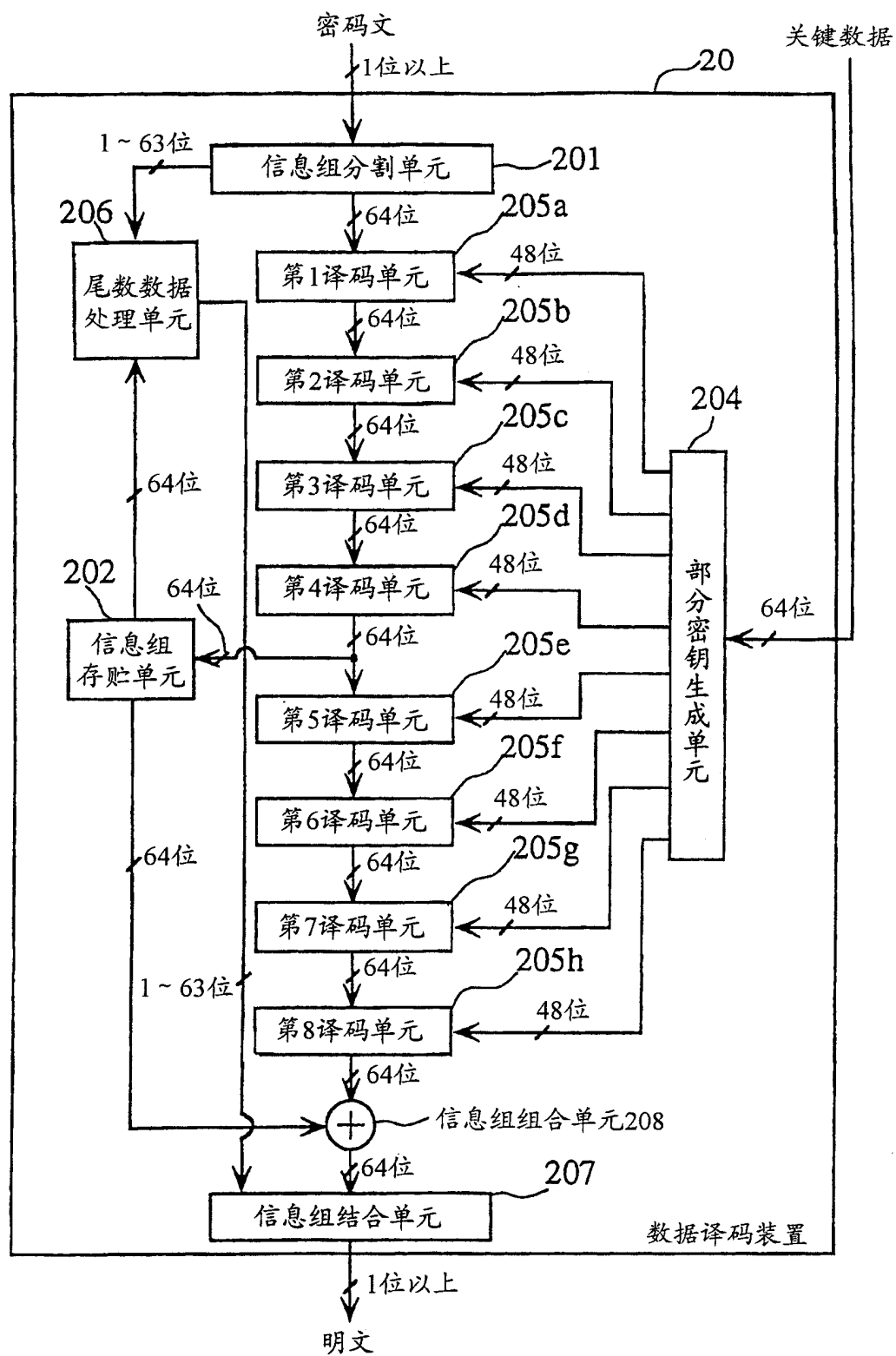


图 13

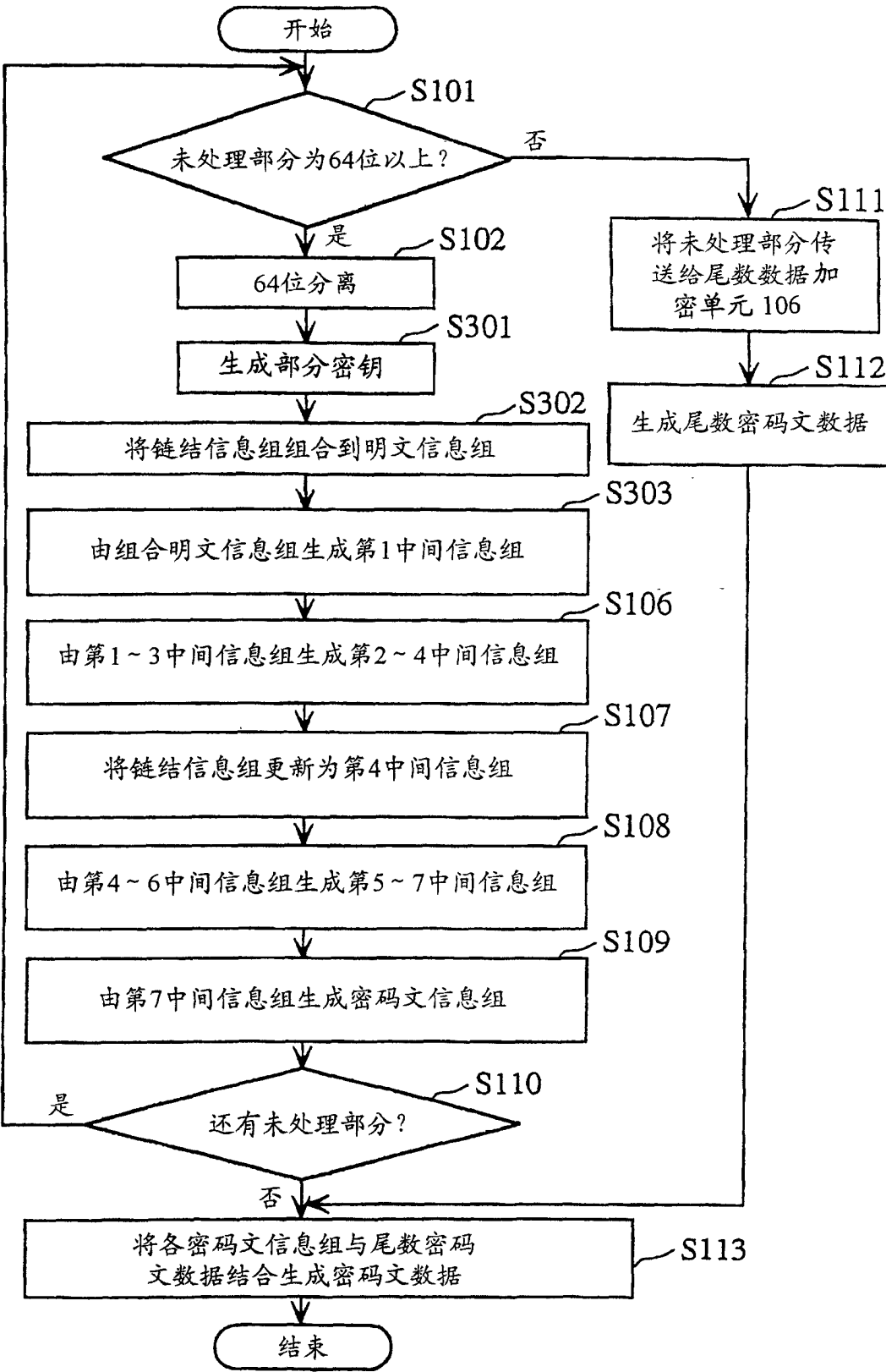


图 14

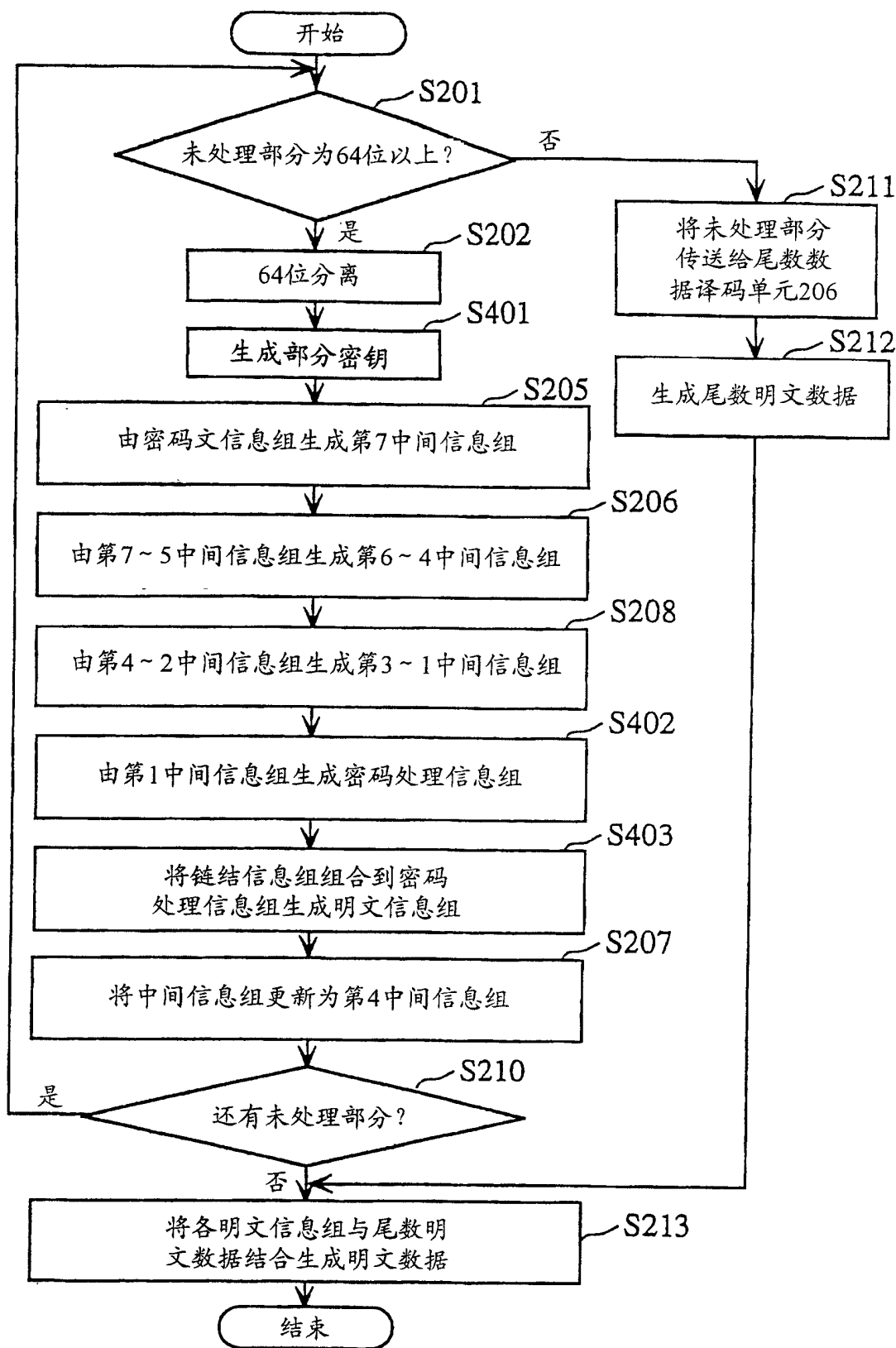


图 15

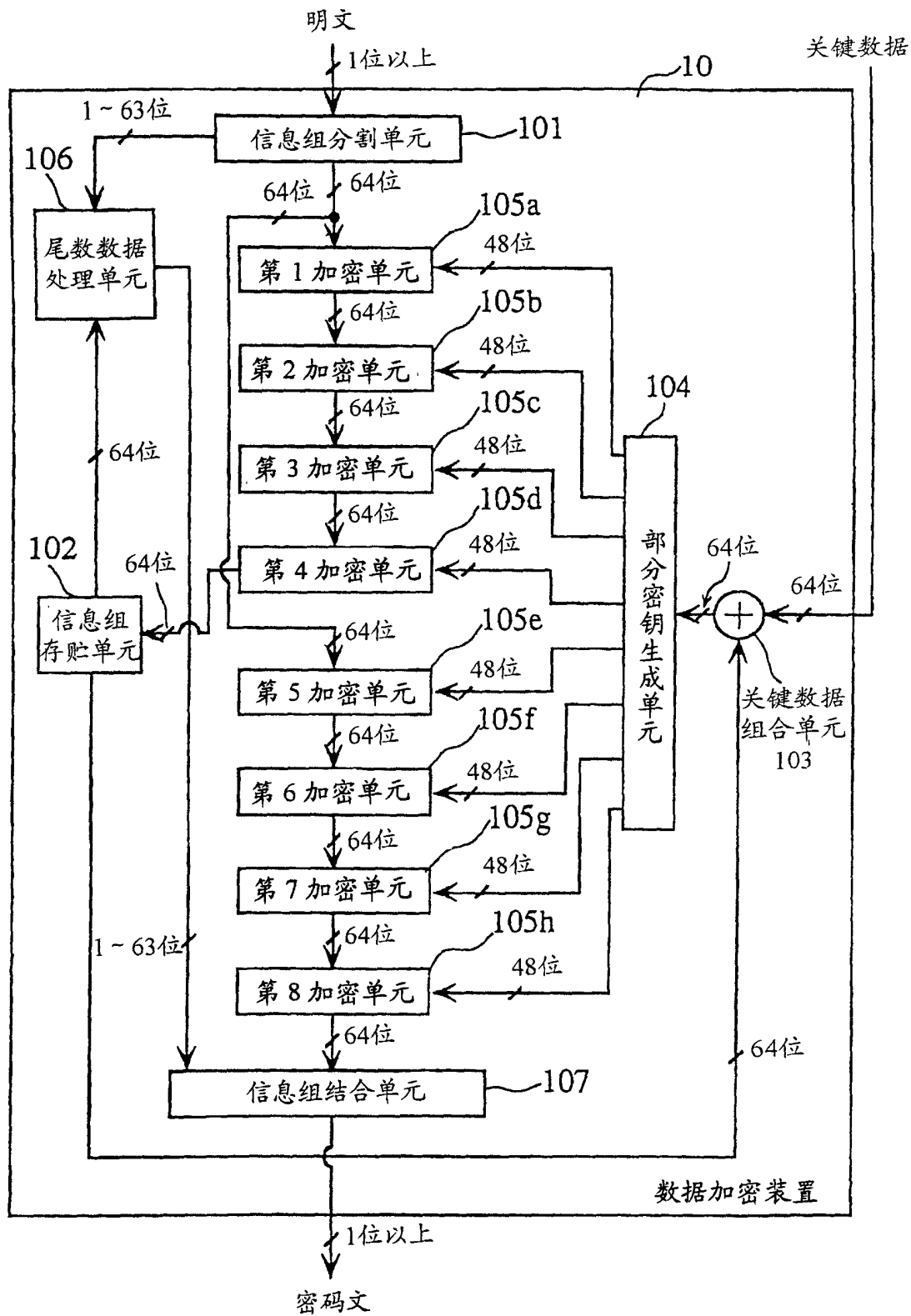


图 16

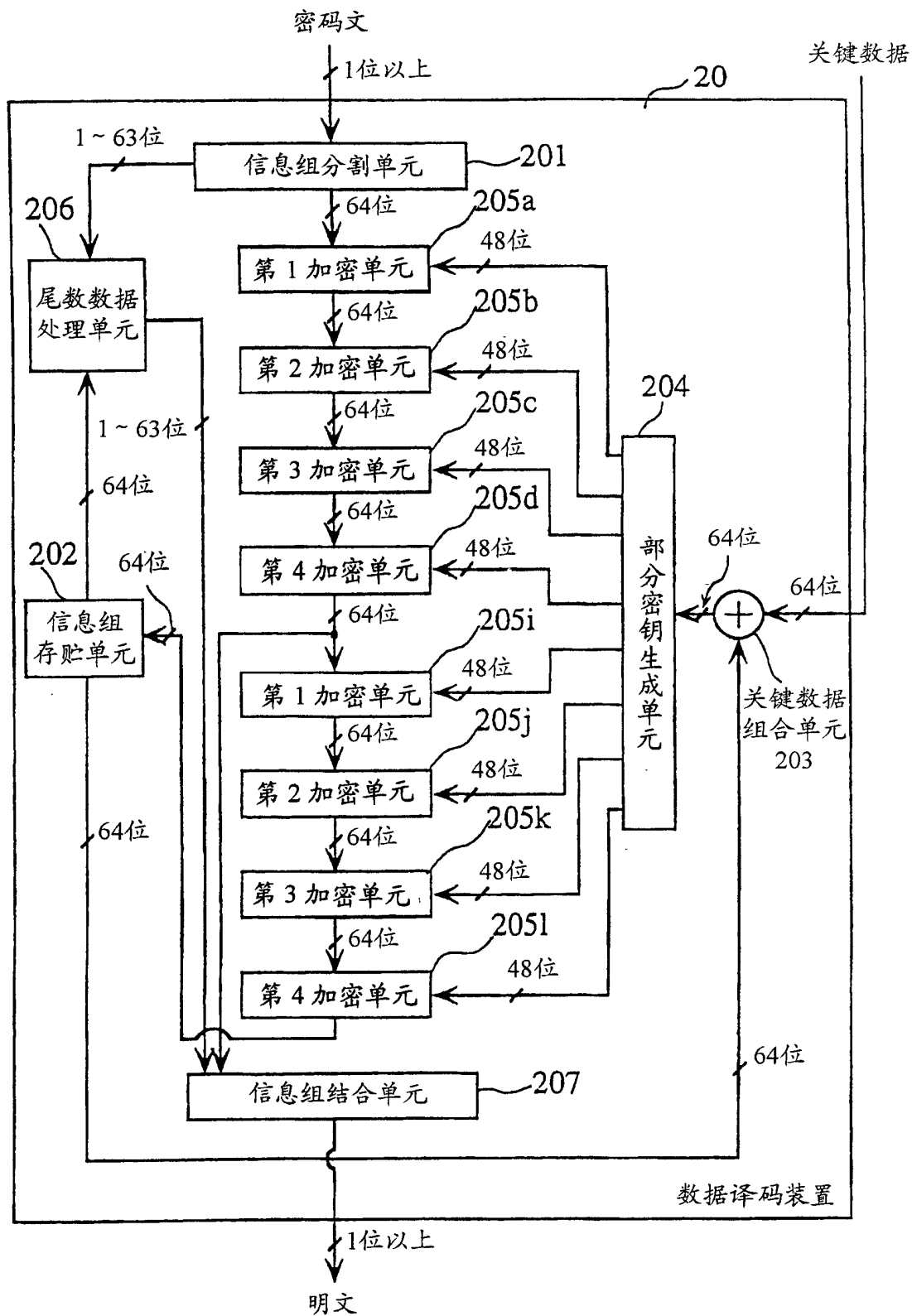


图 17

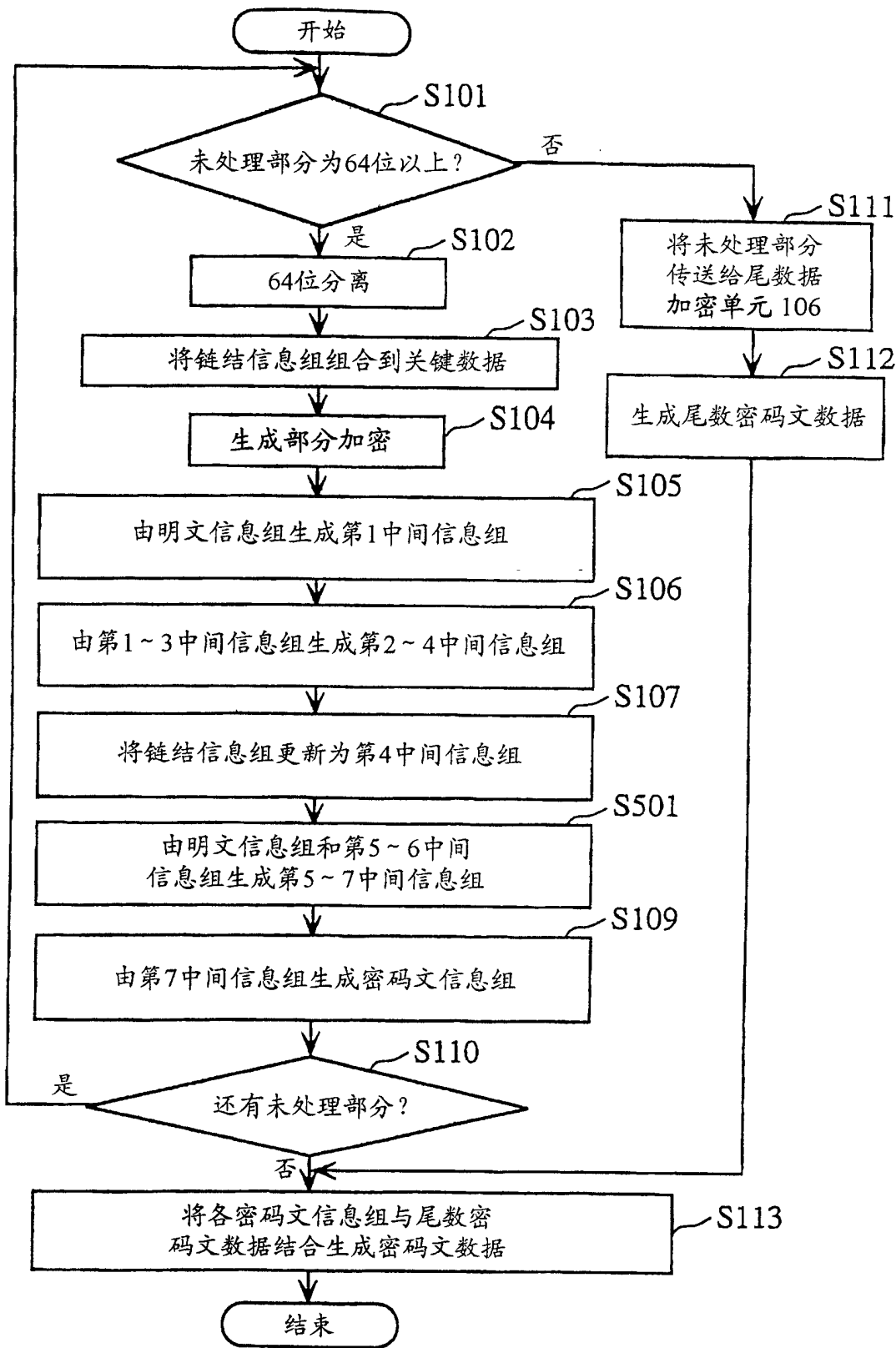


图 18

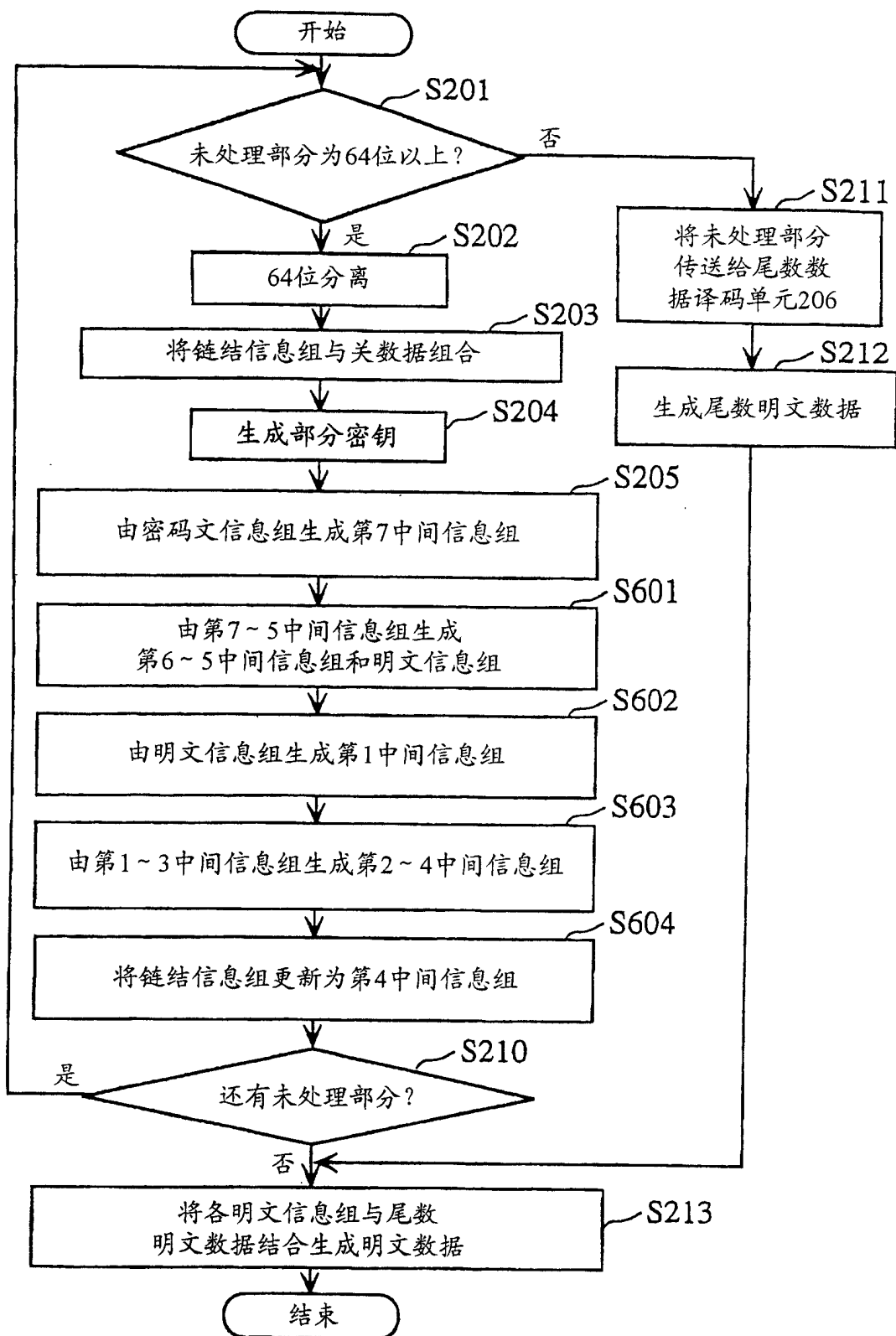
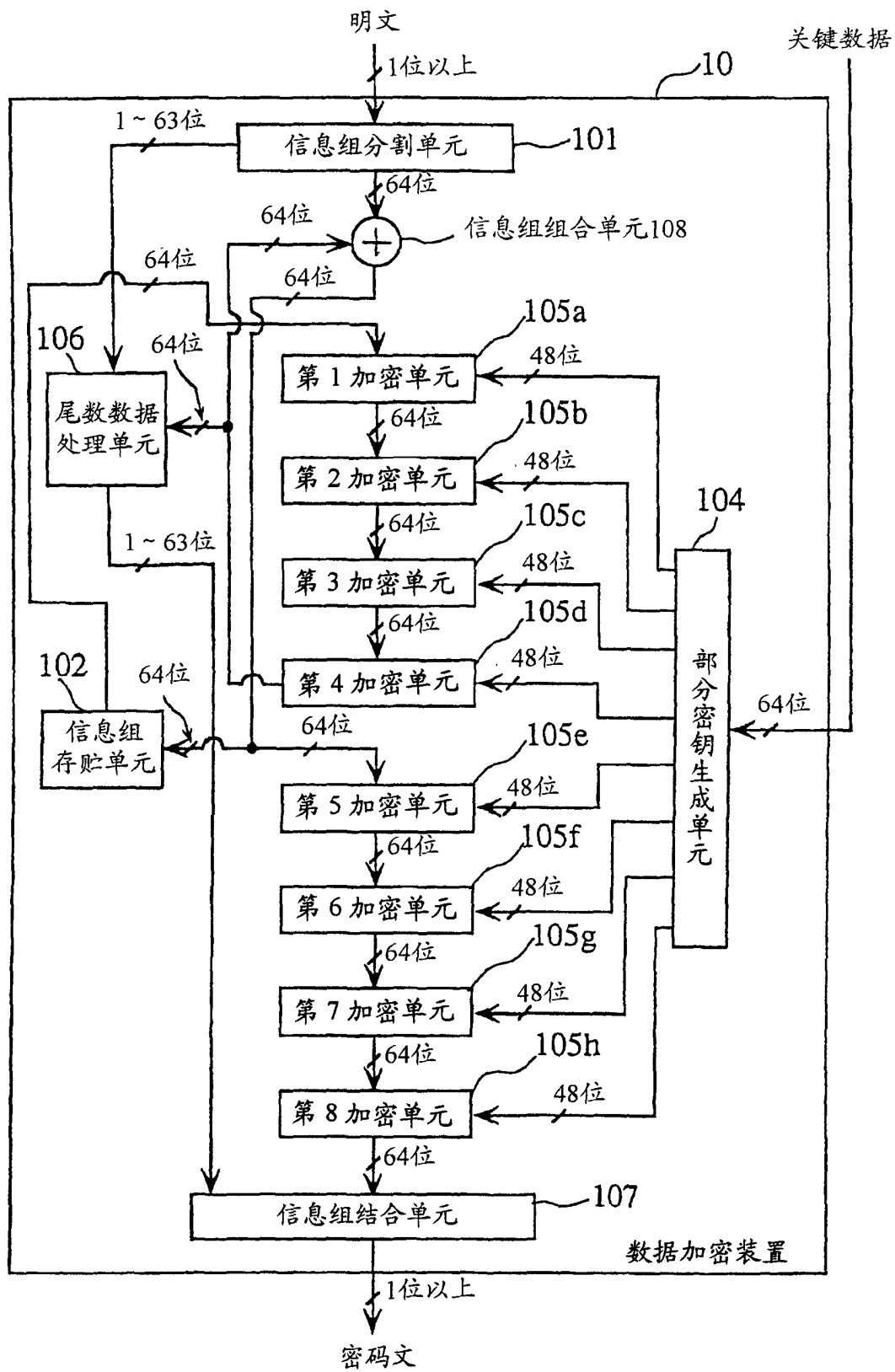


图 19



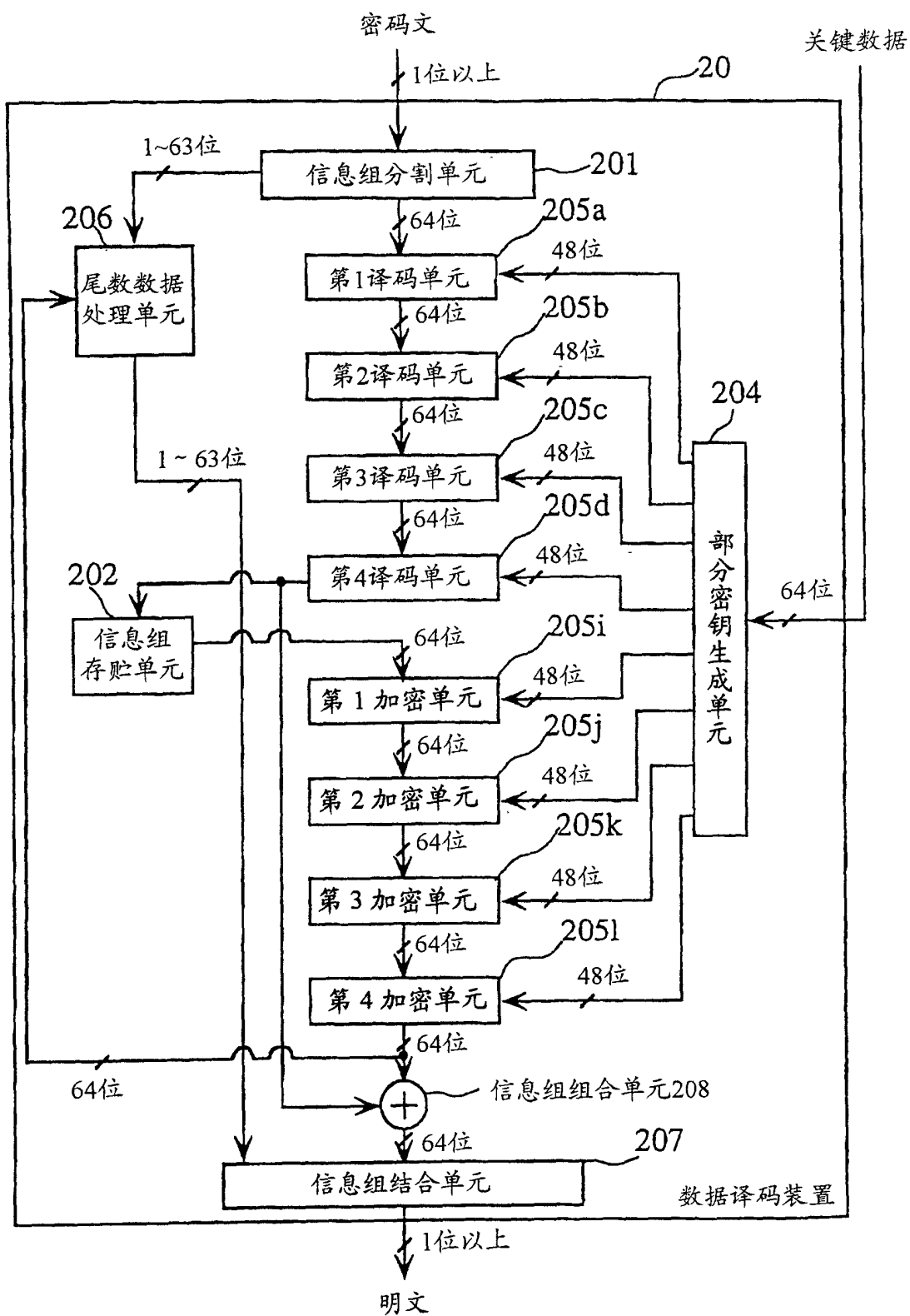


图 21

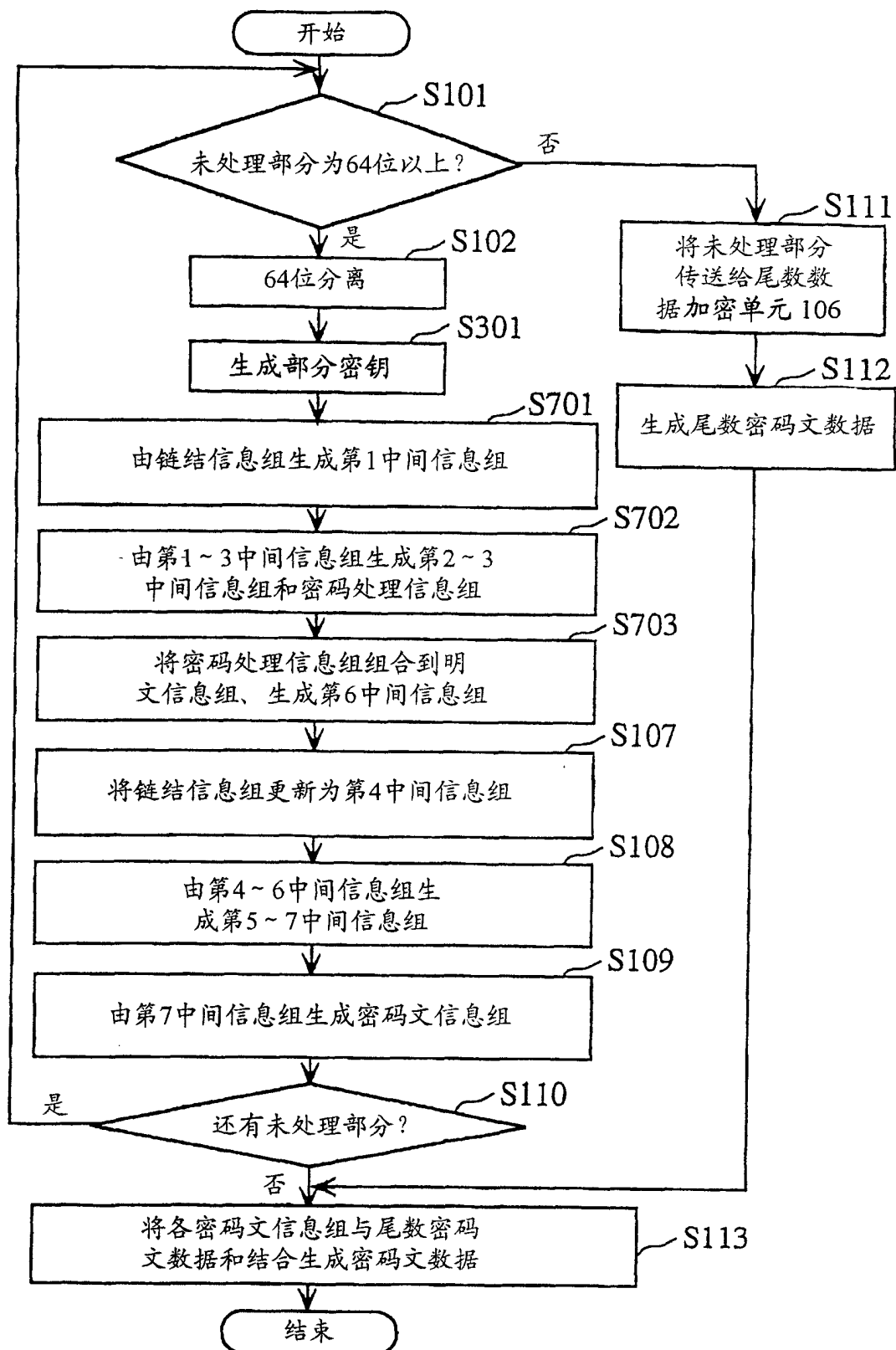


图 22

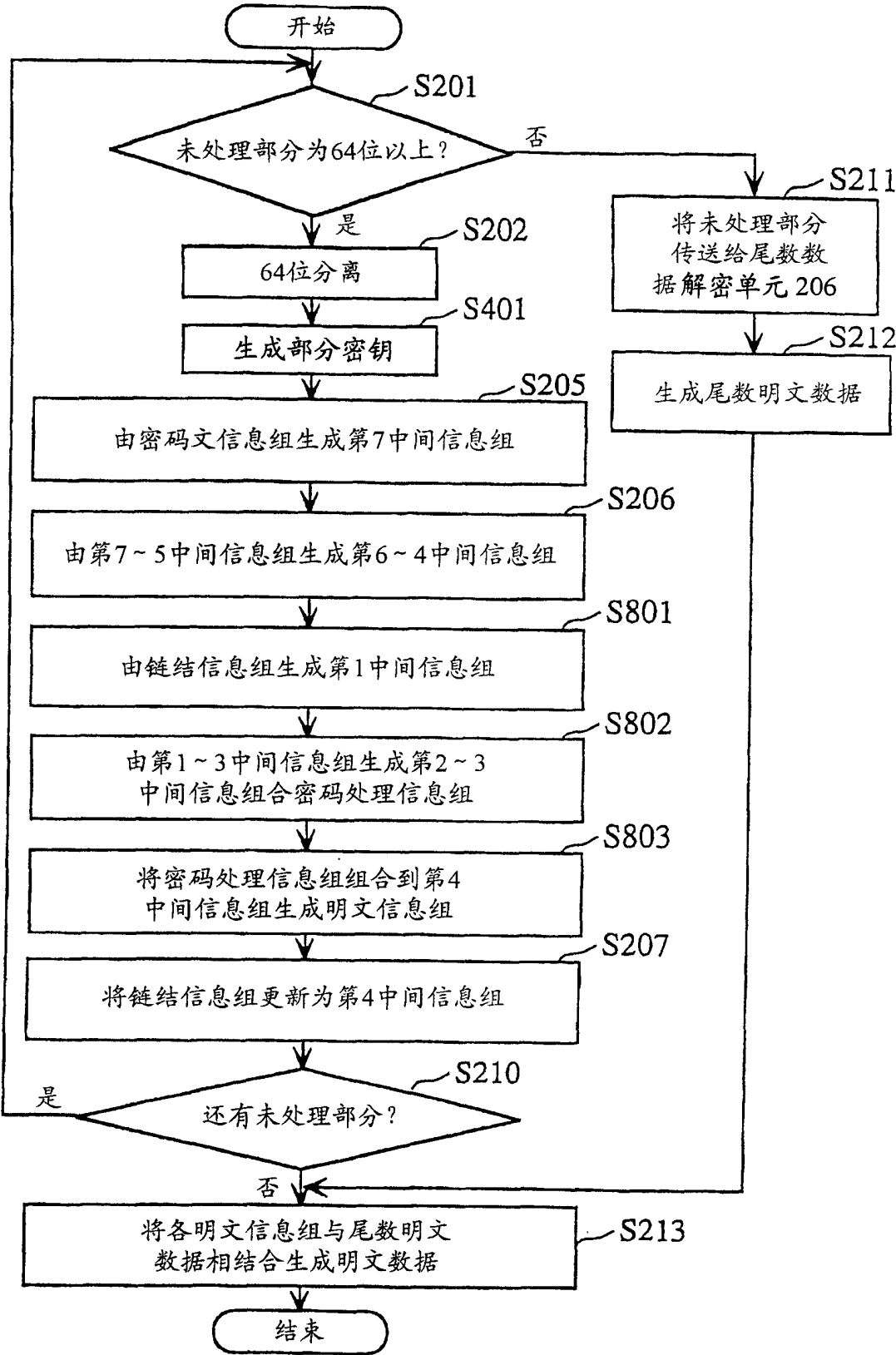


图 23

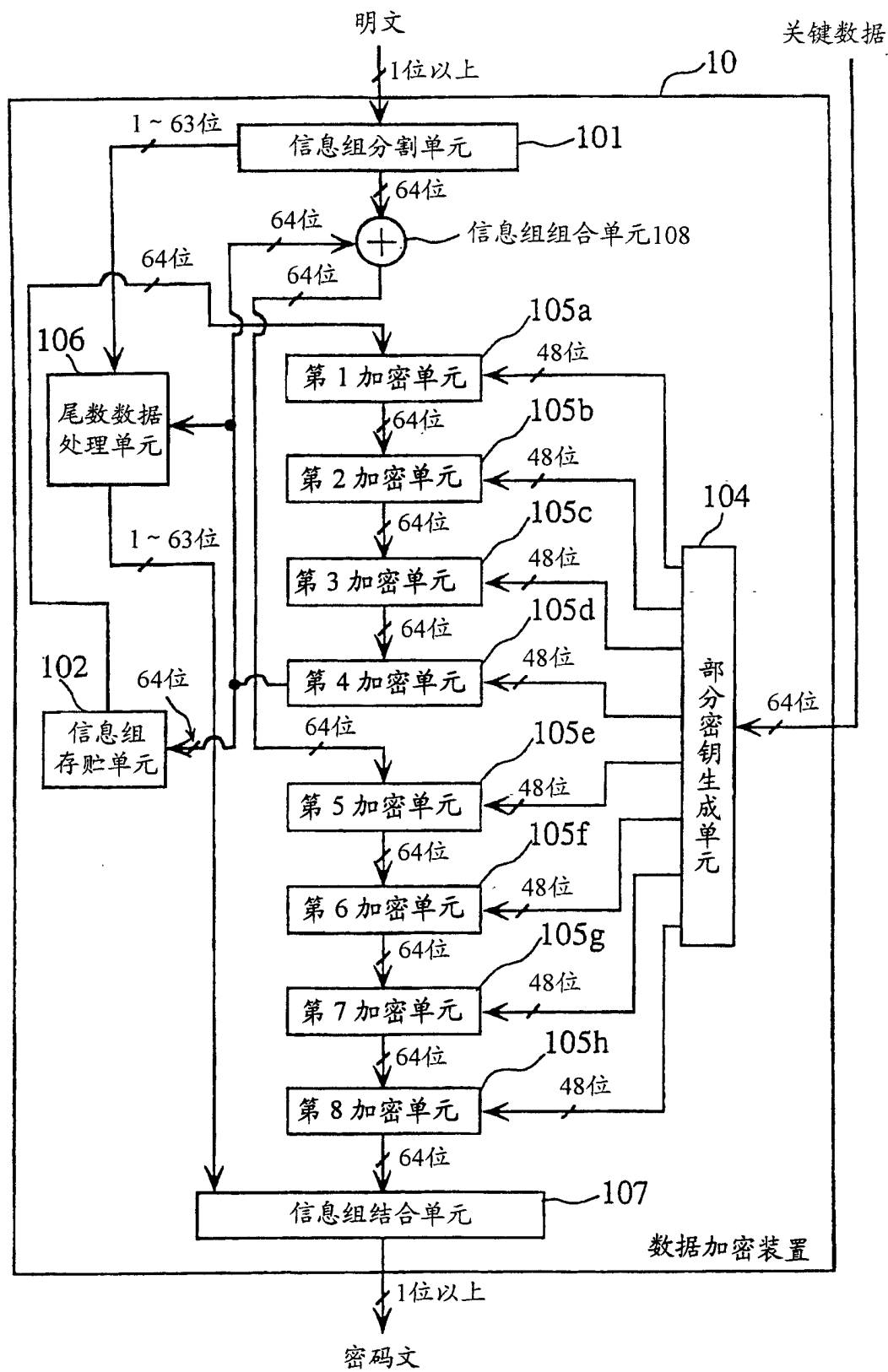


图 24

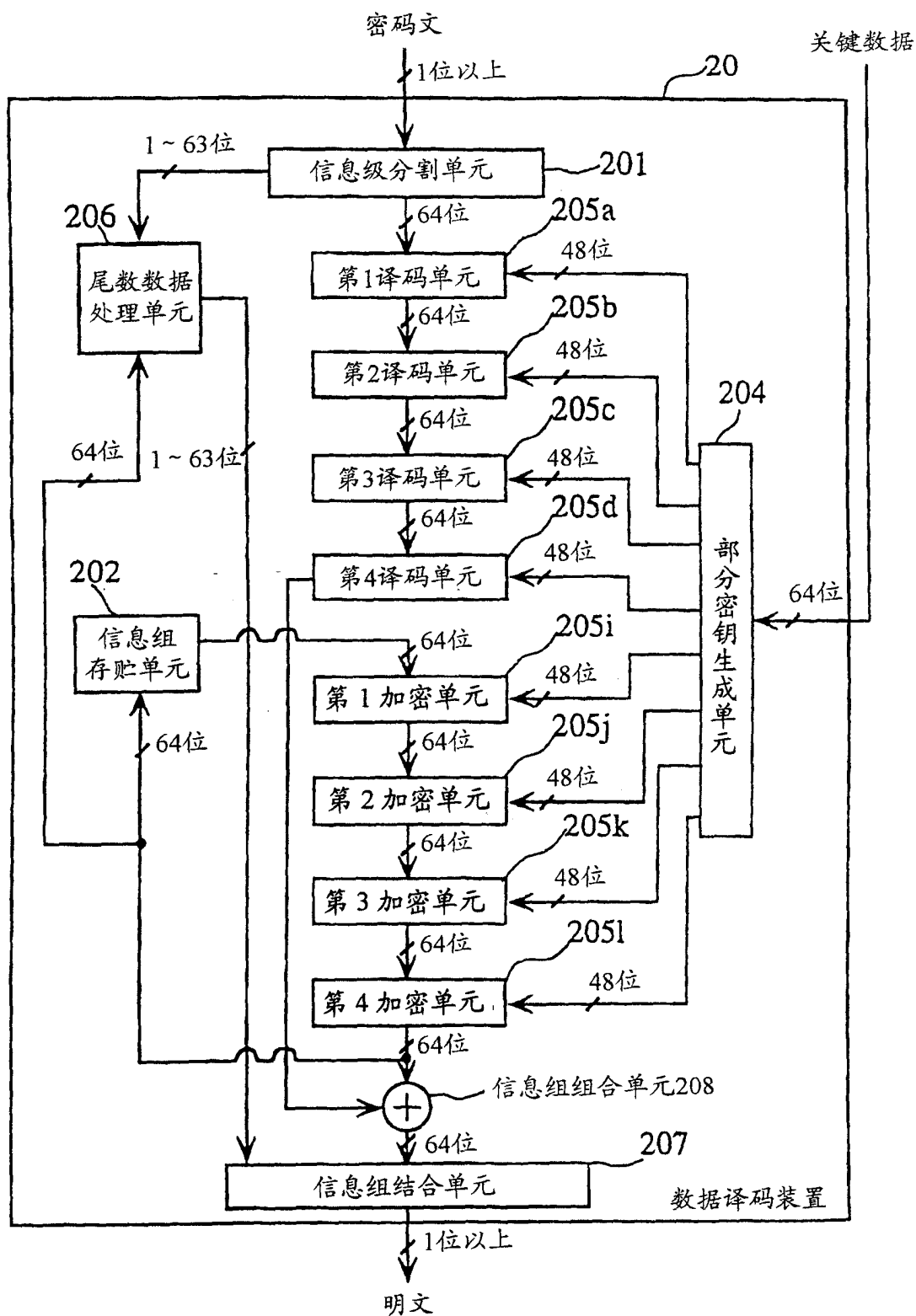


图 25

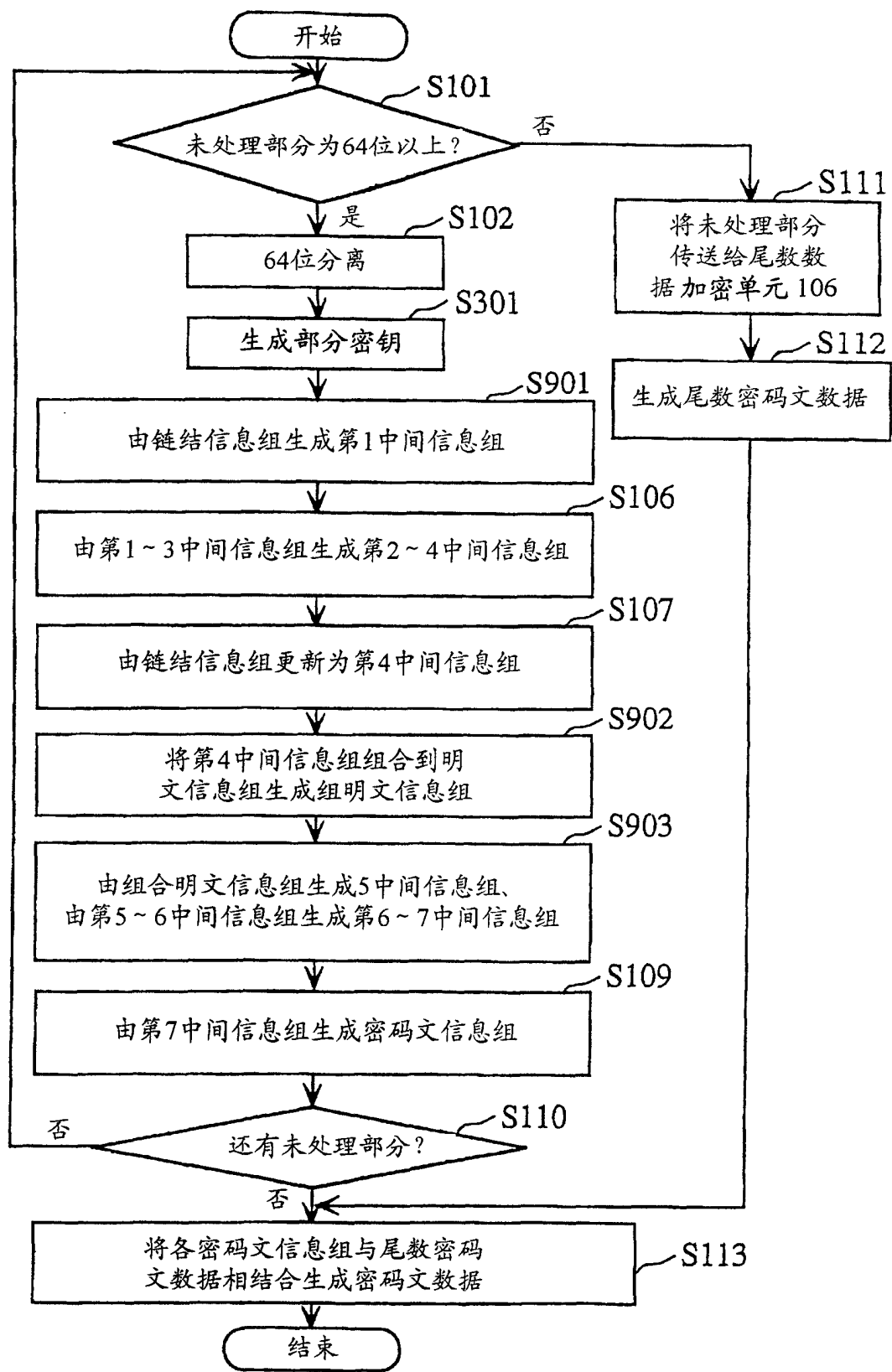


图 26

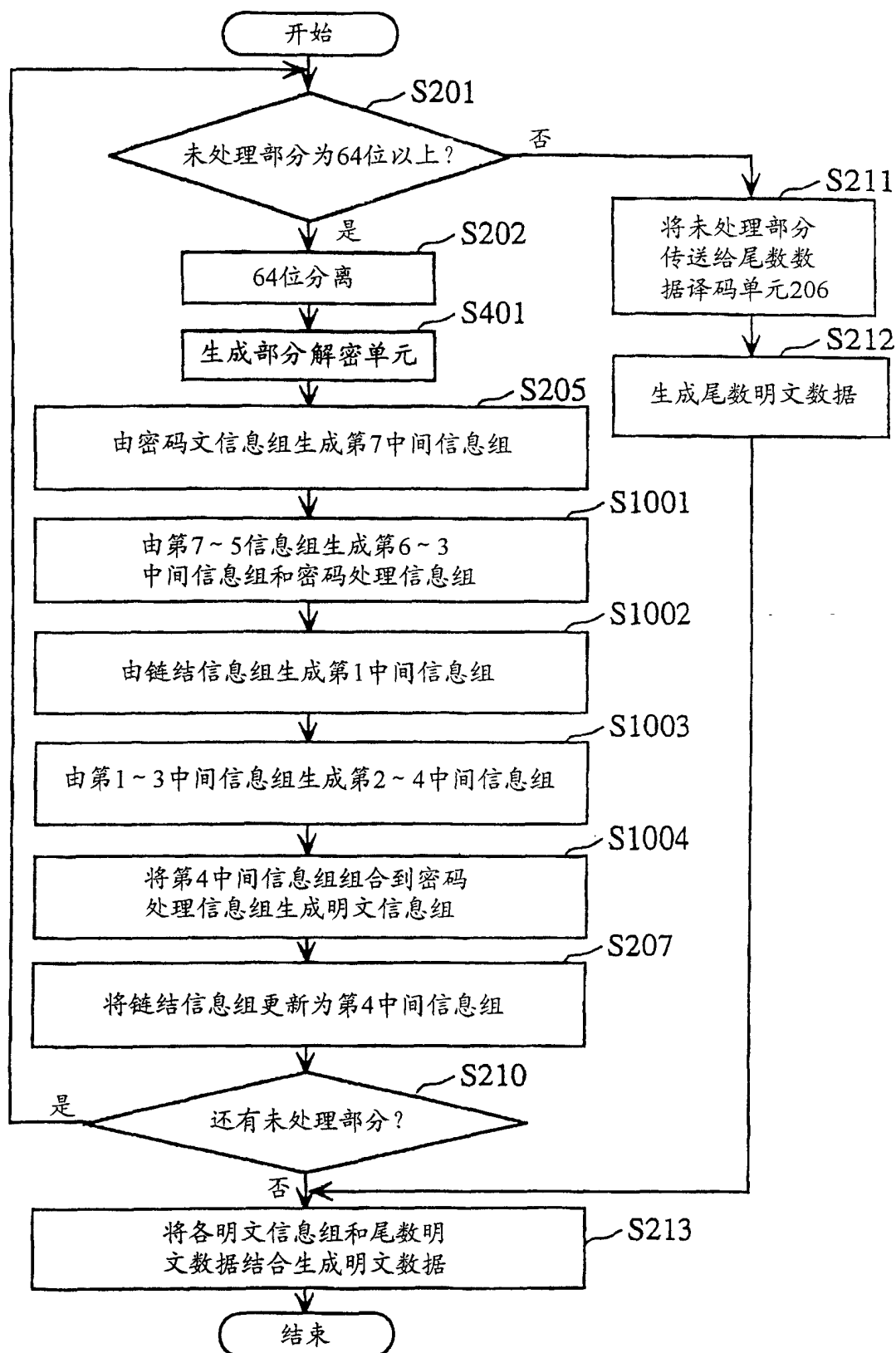


图 27

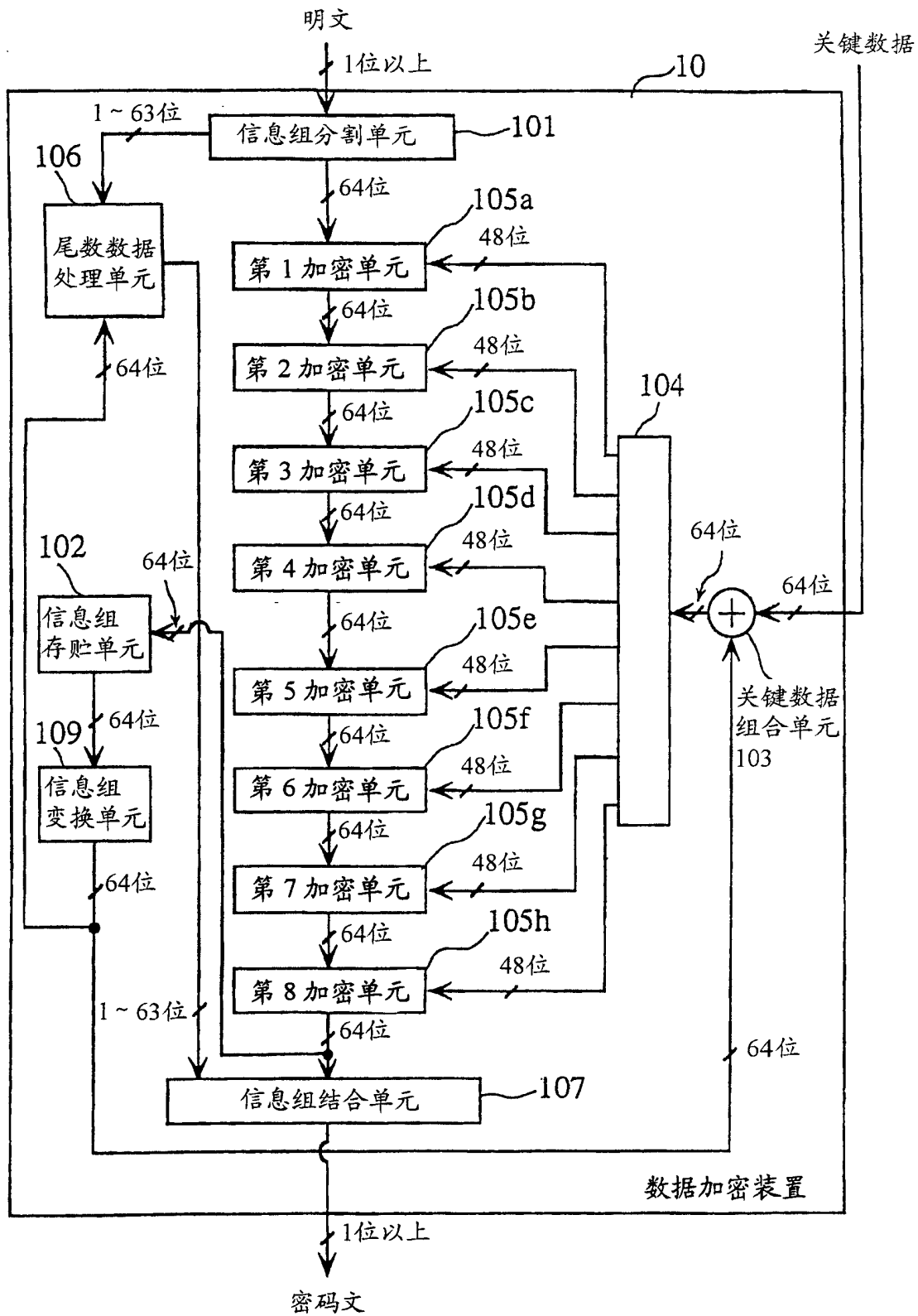


图 28

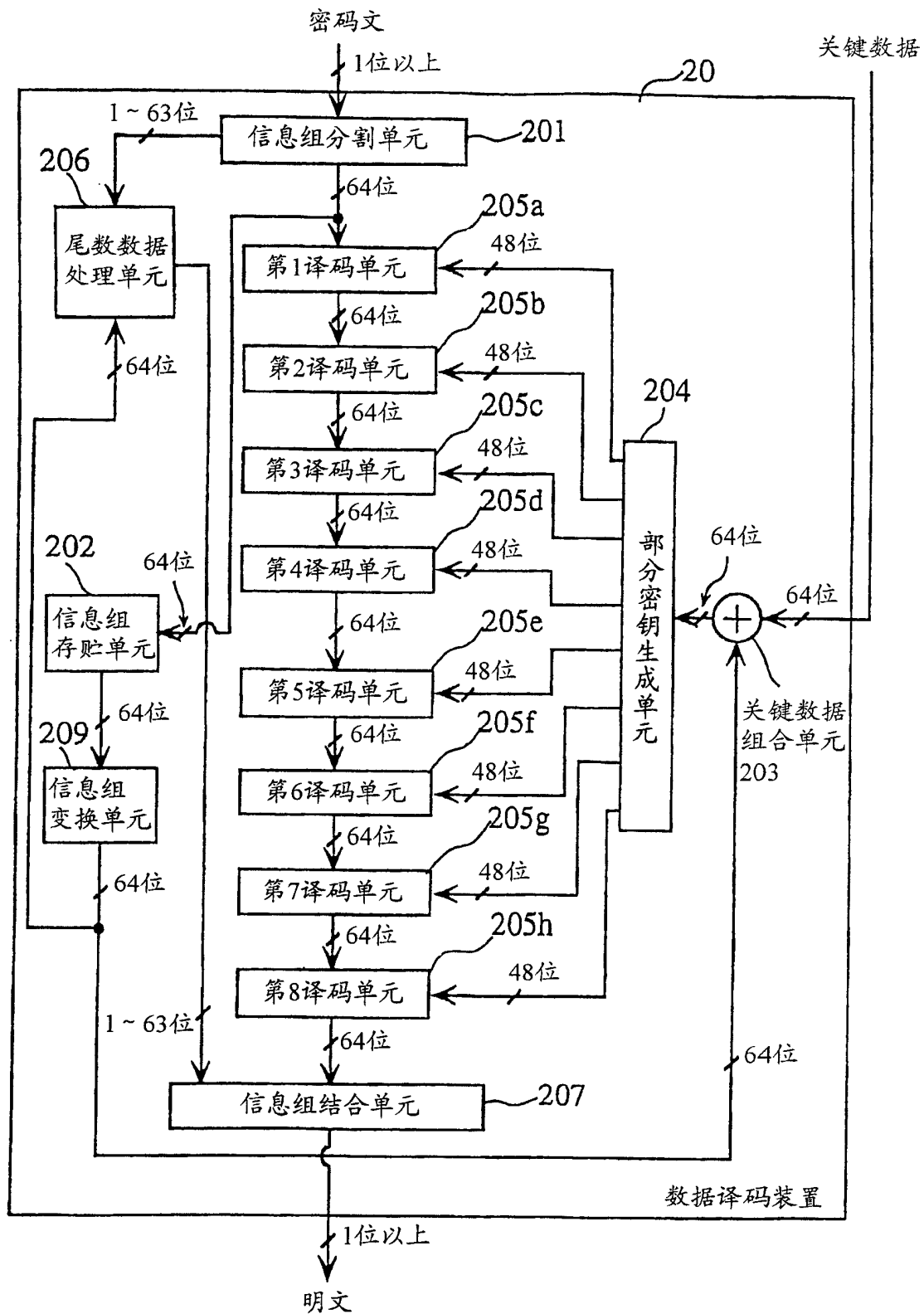


图 29

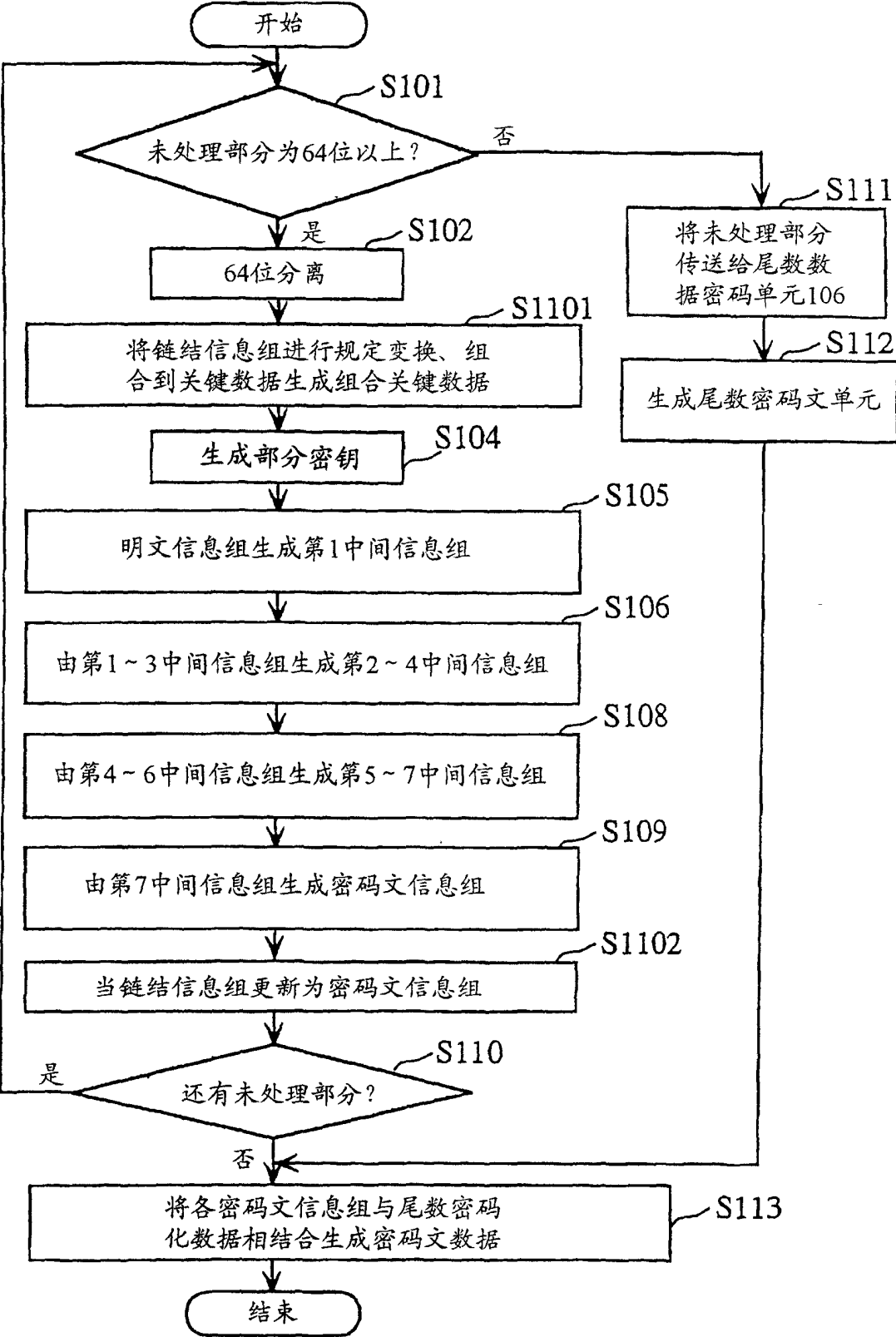


图 30

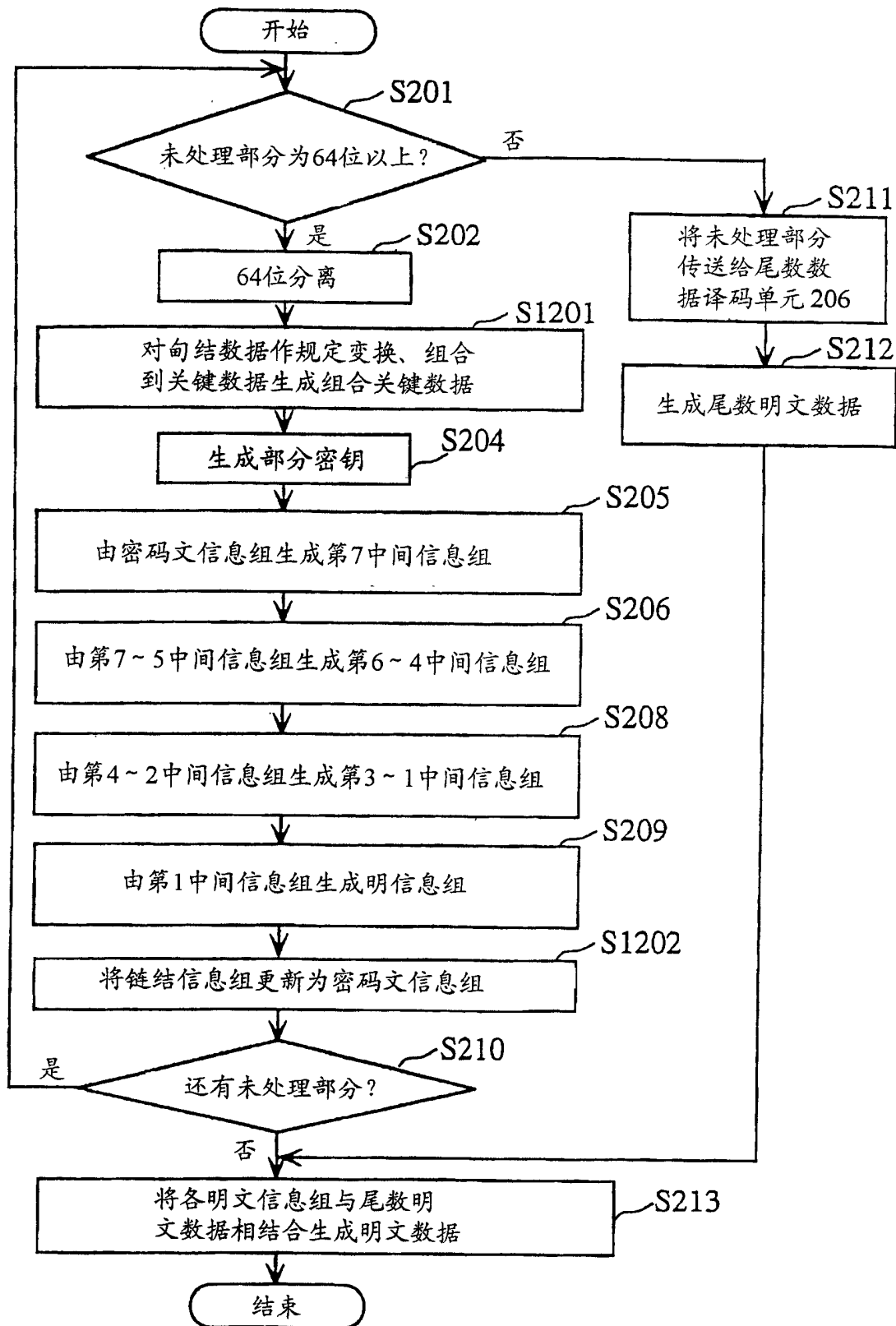


图 31

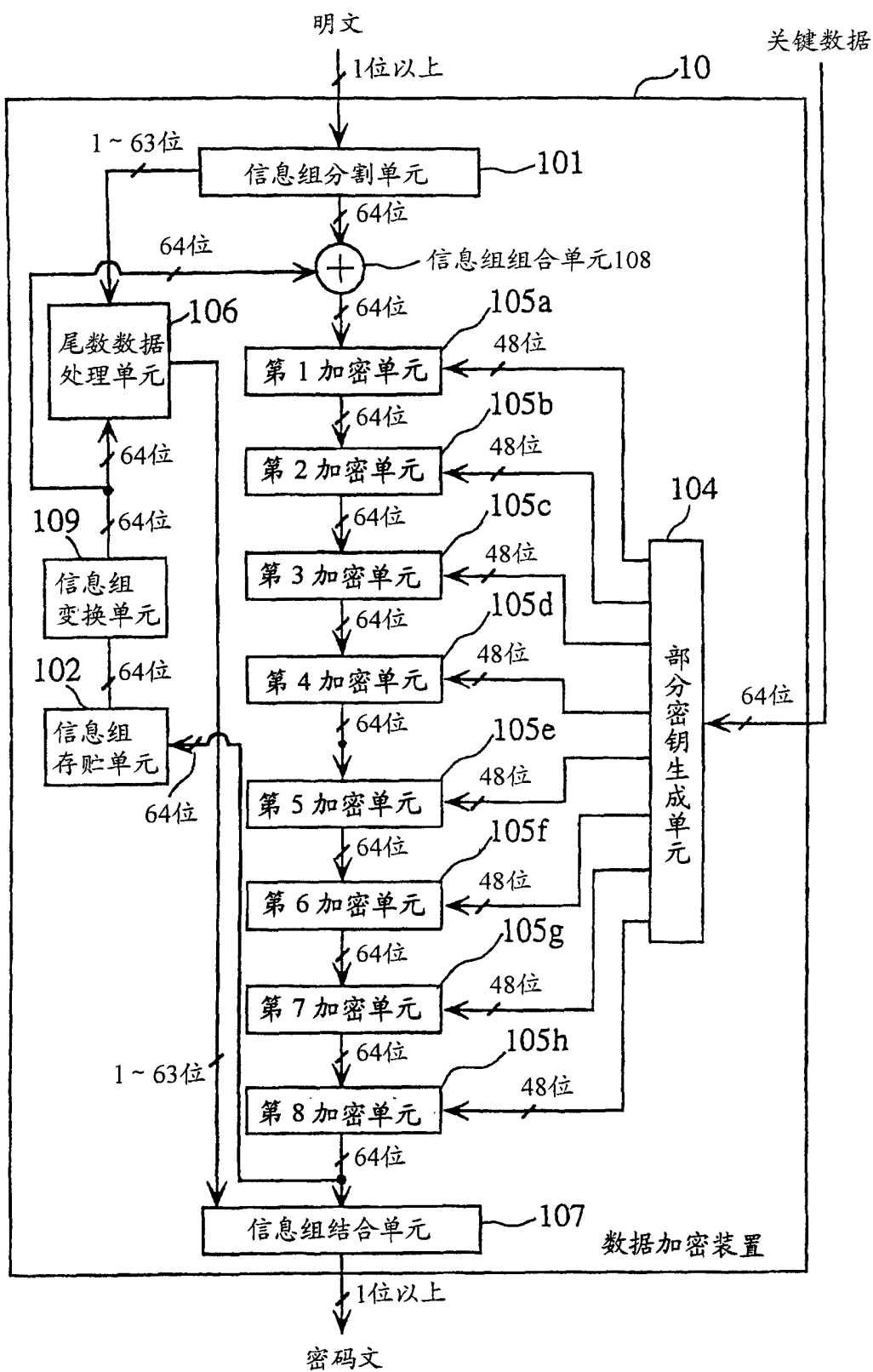


图 32

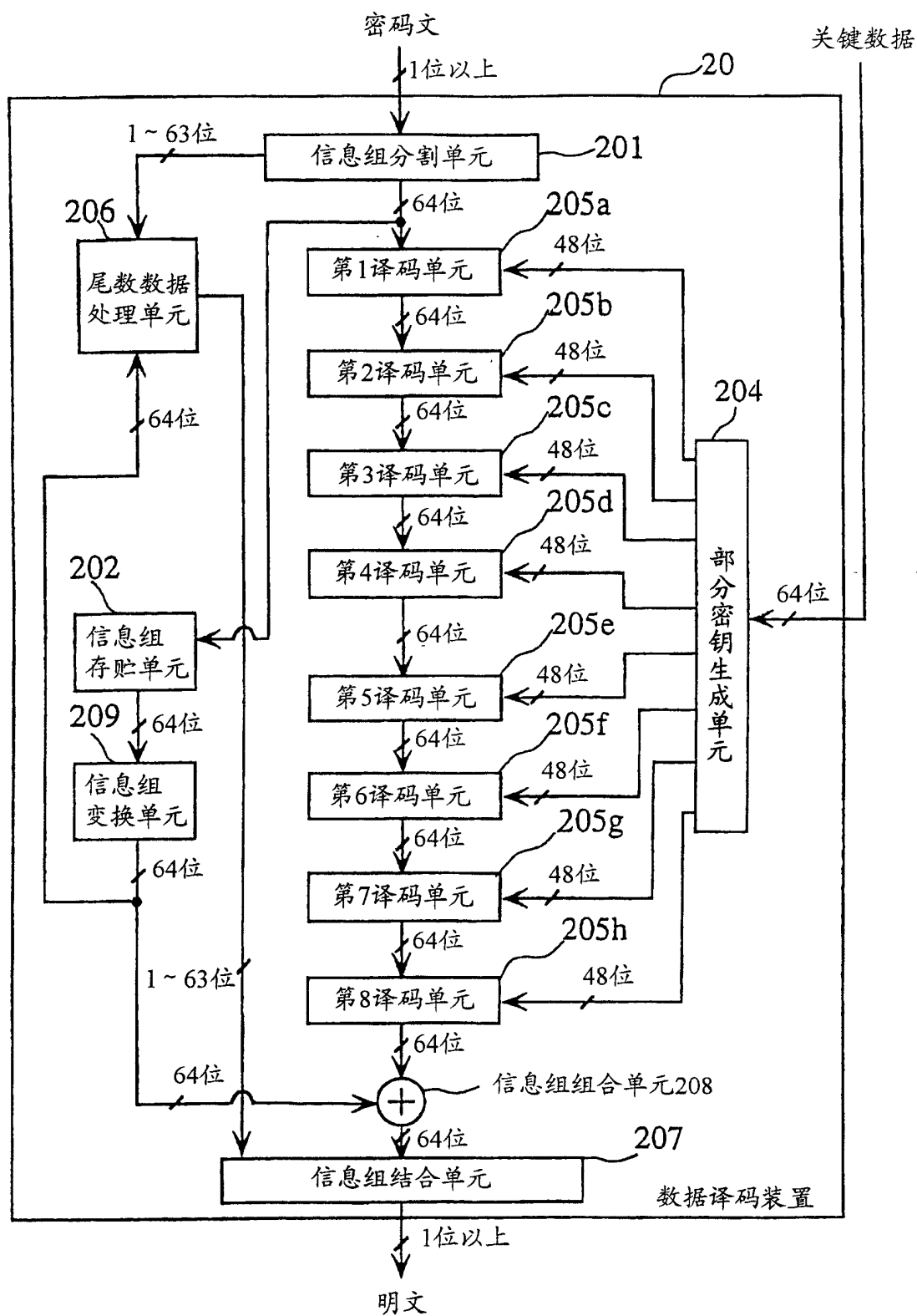


图 33

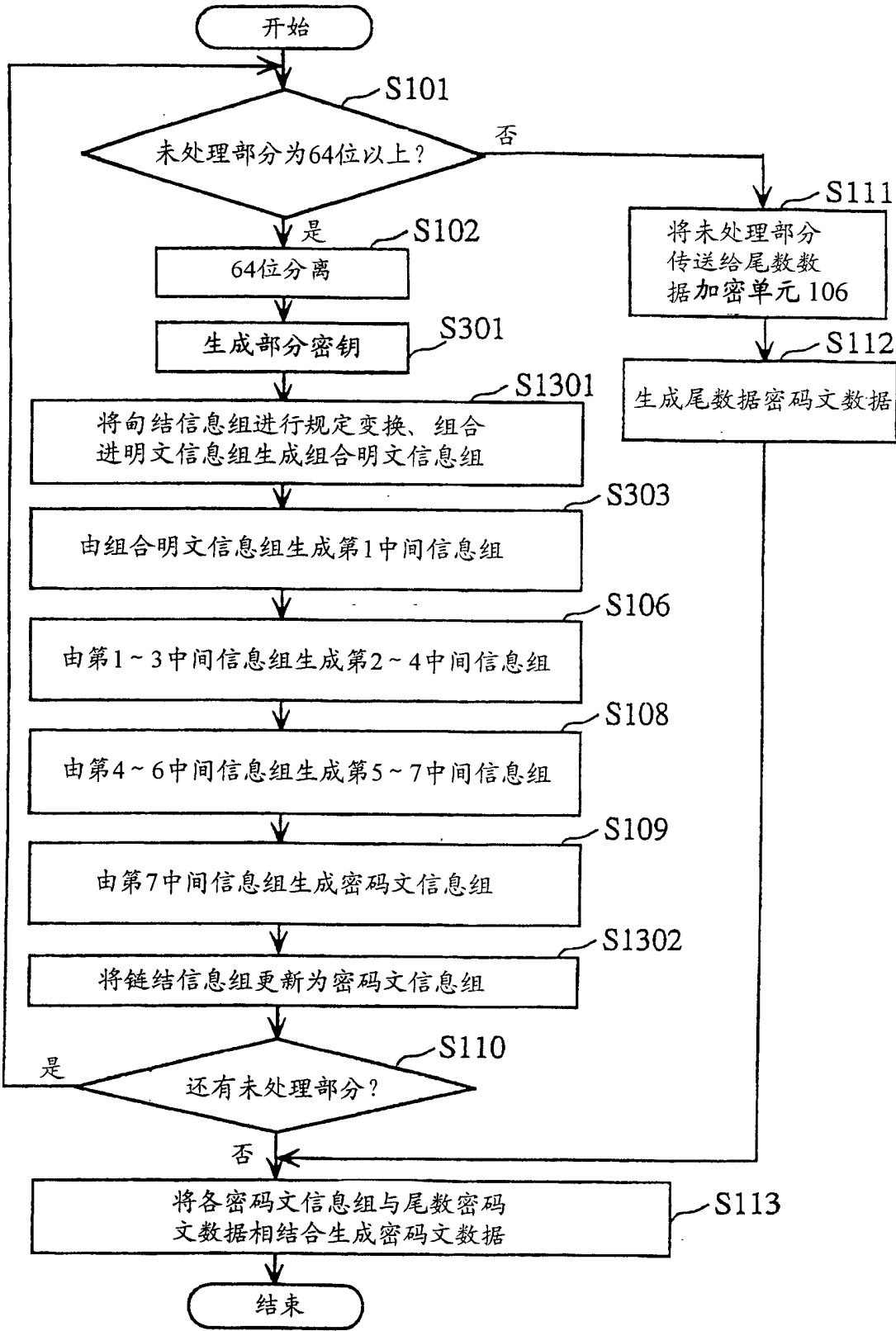


图 34

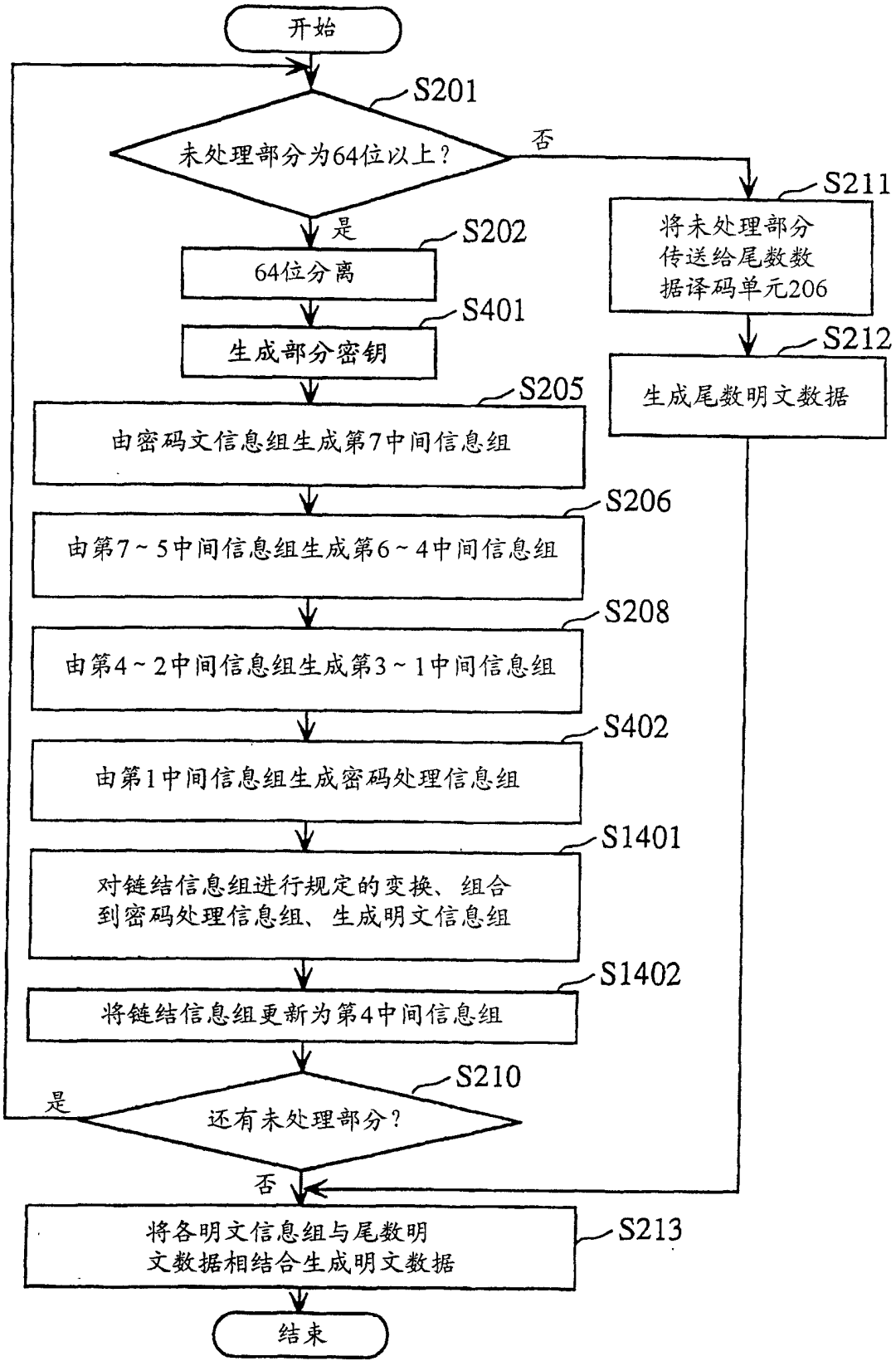


图 35

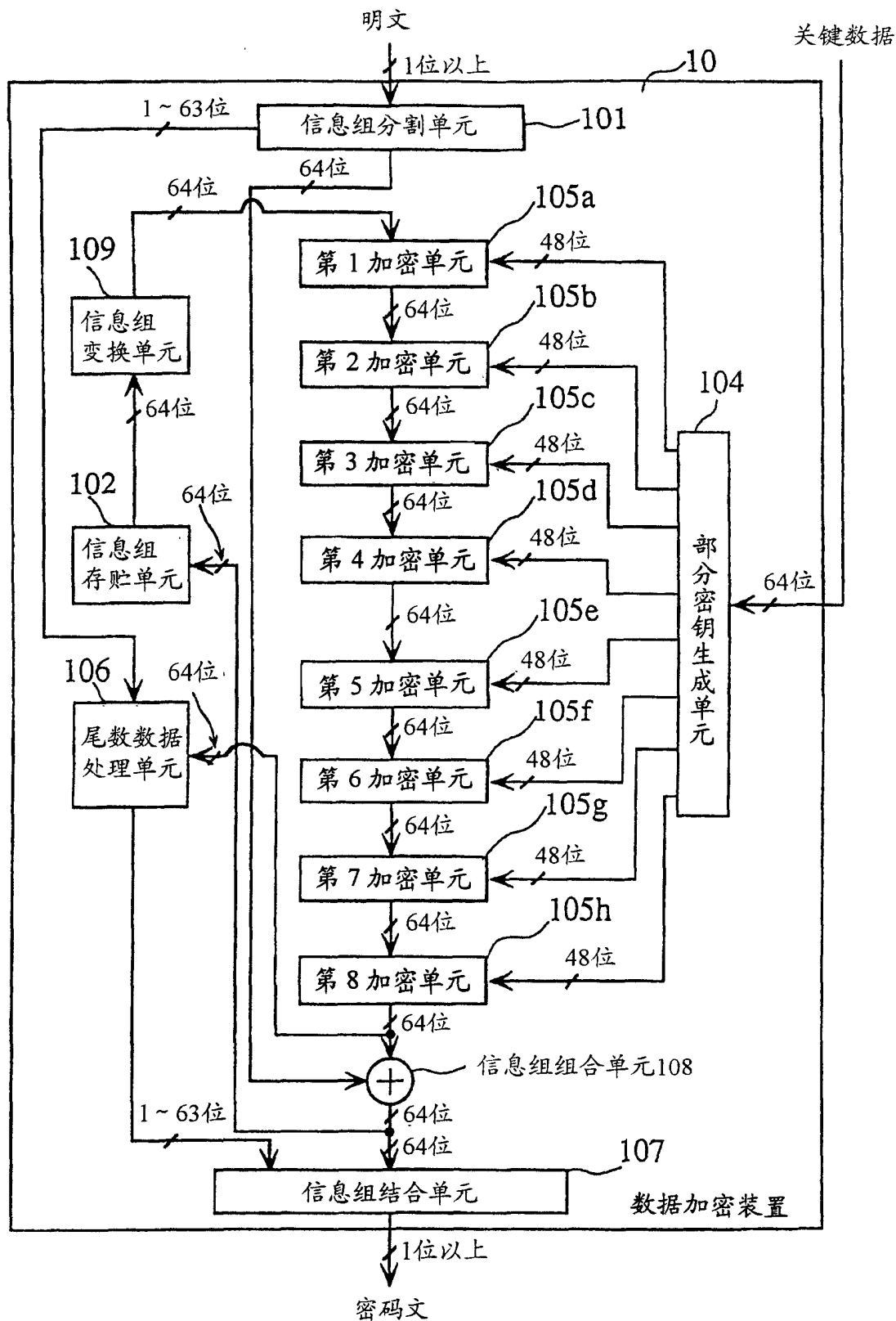


图 36

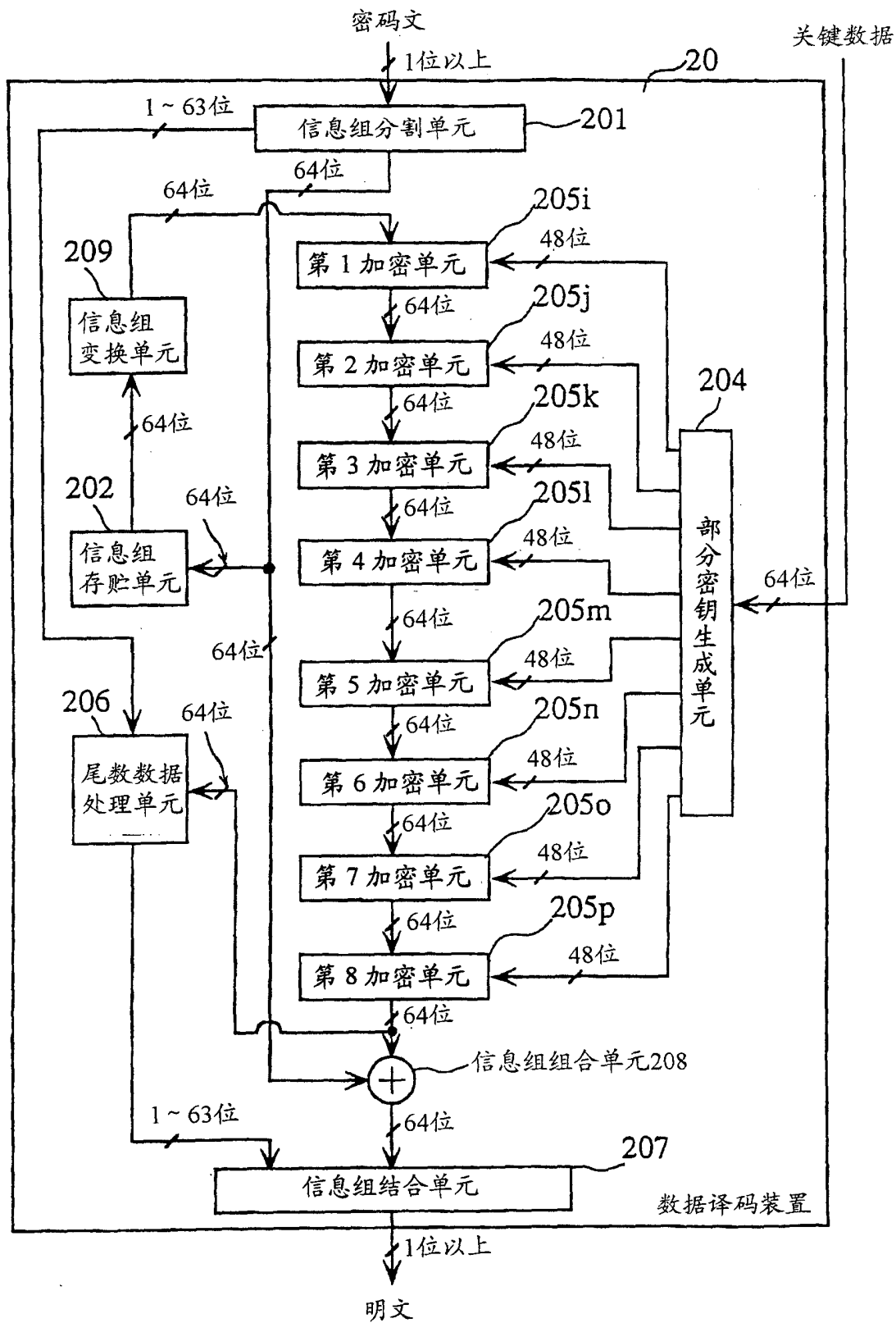


图 37

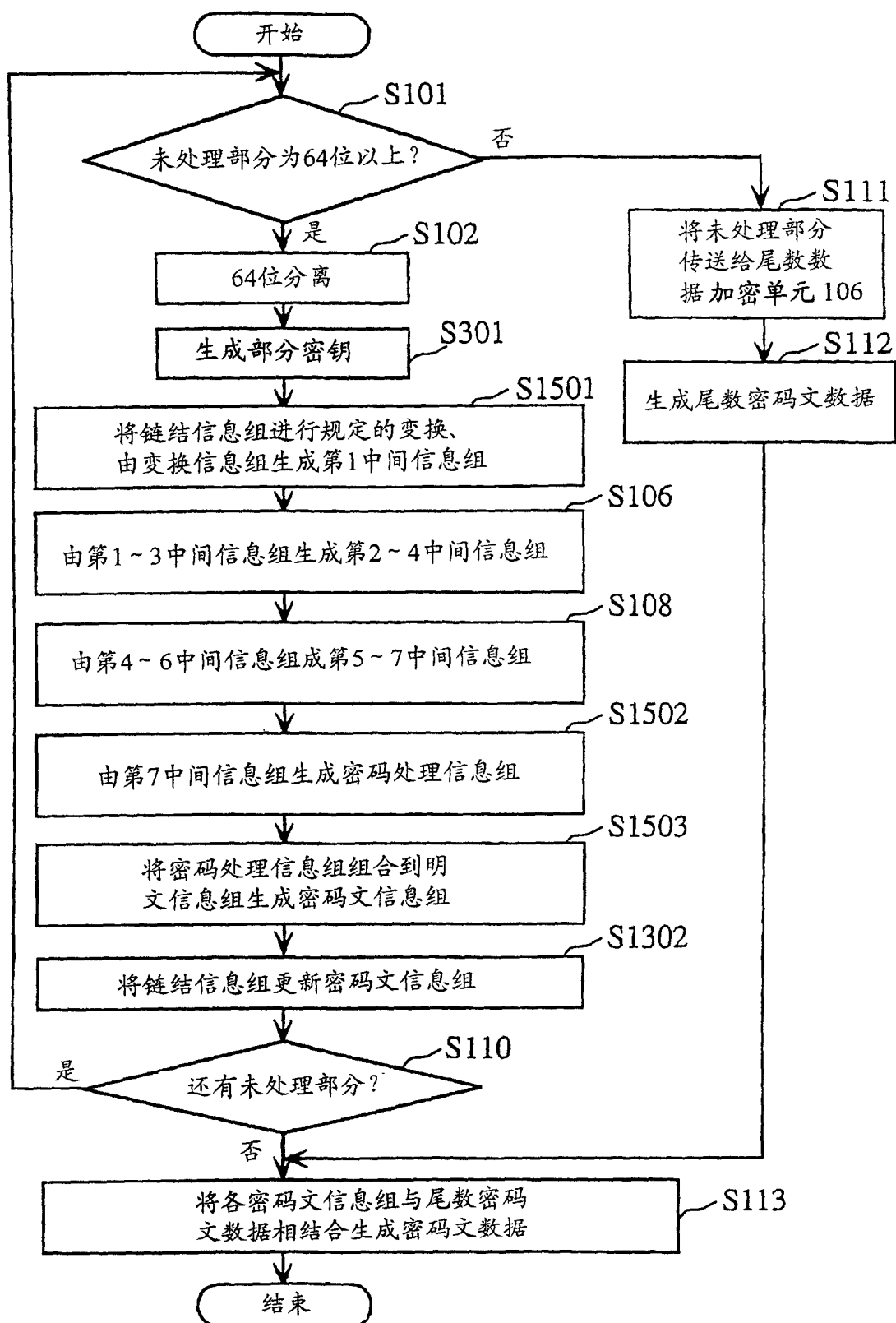


图 38

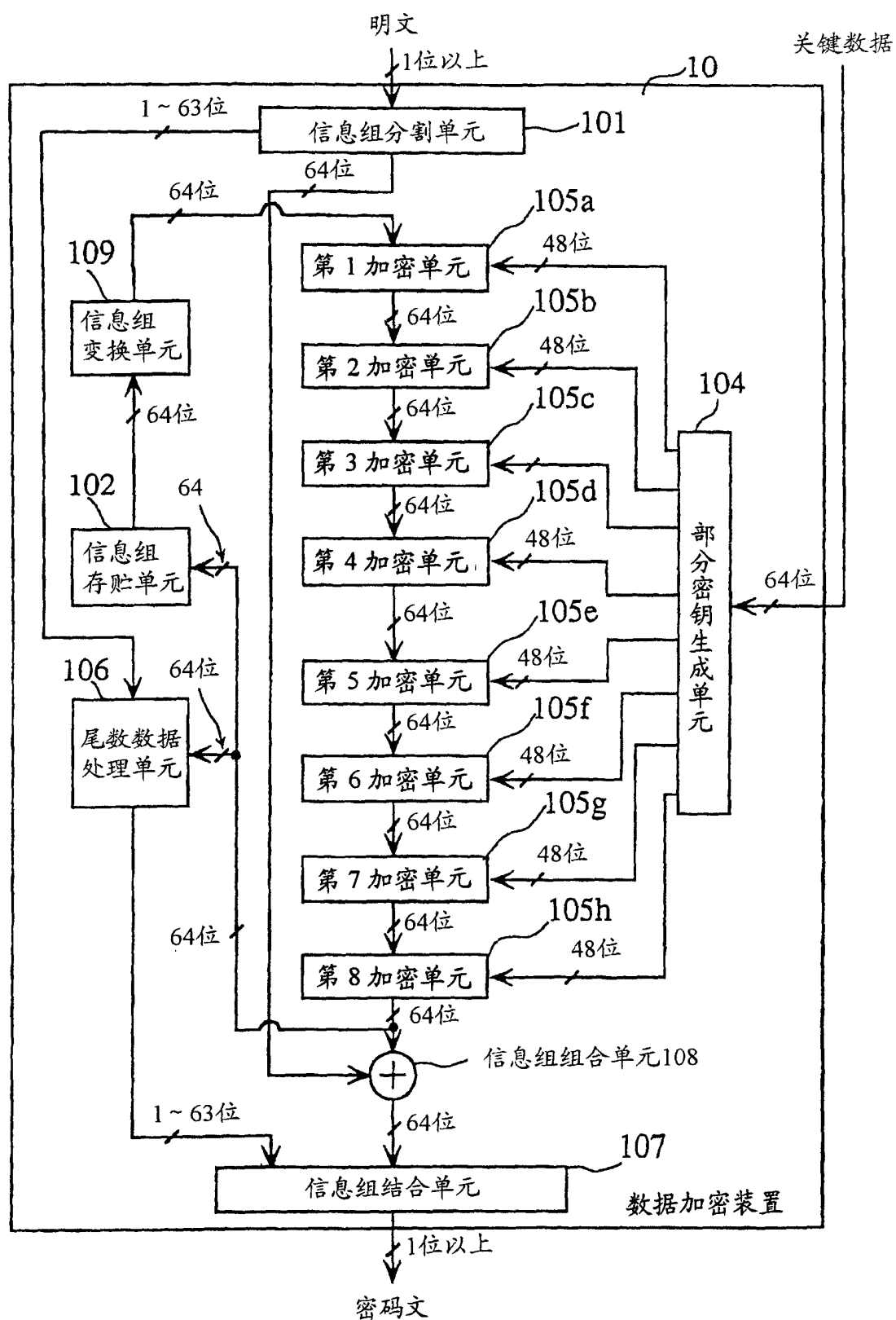


图 39

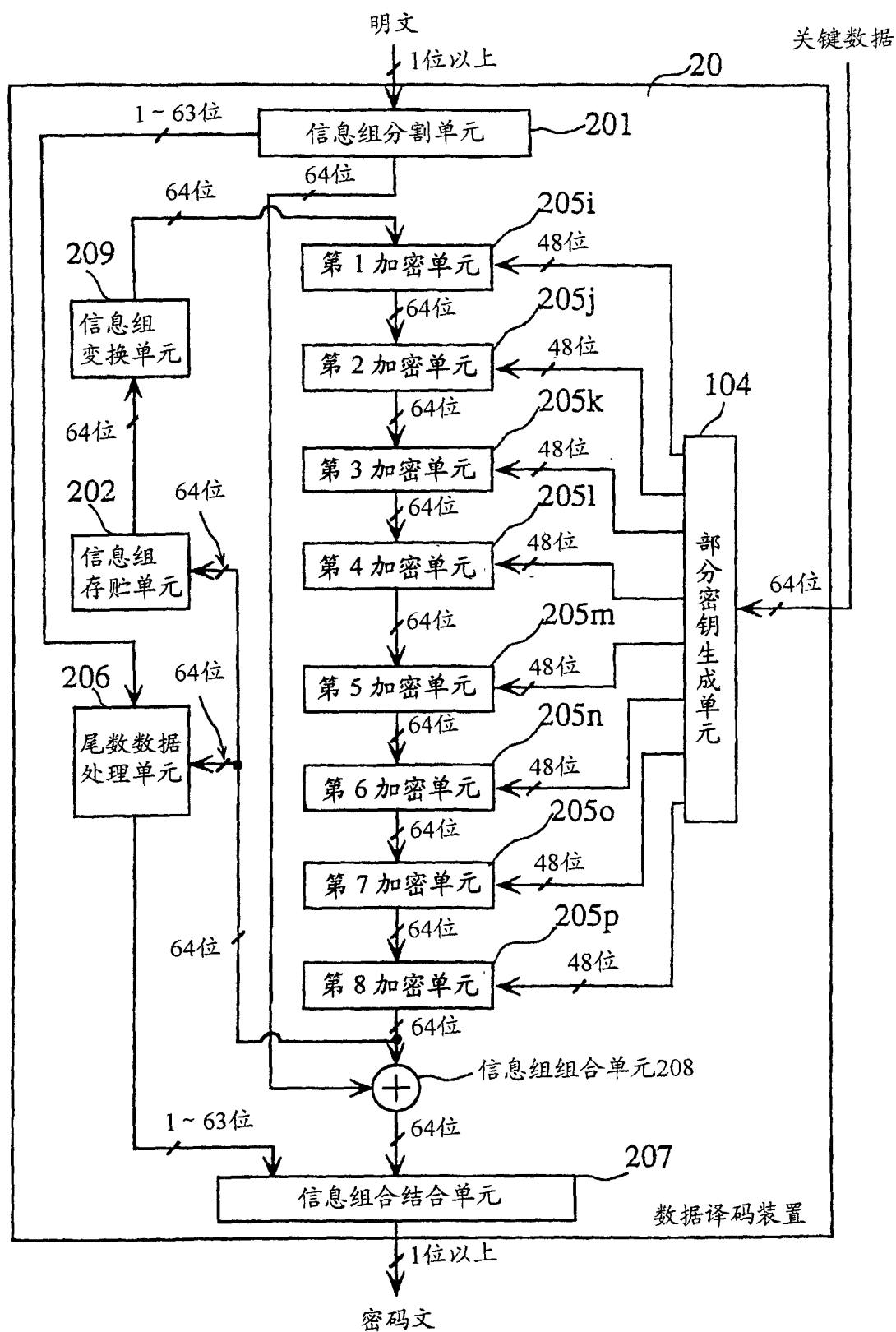


图 40

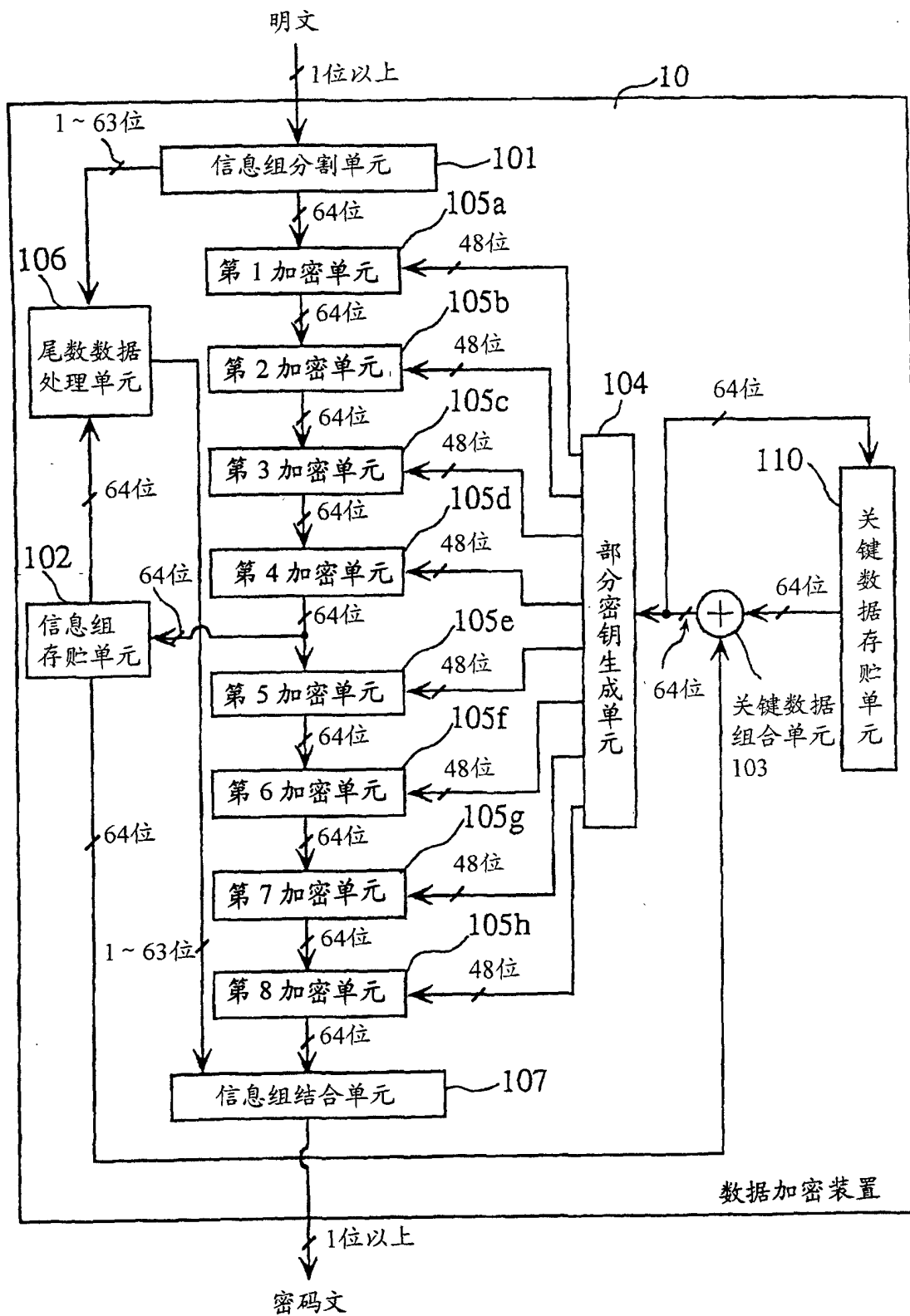


图 41

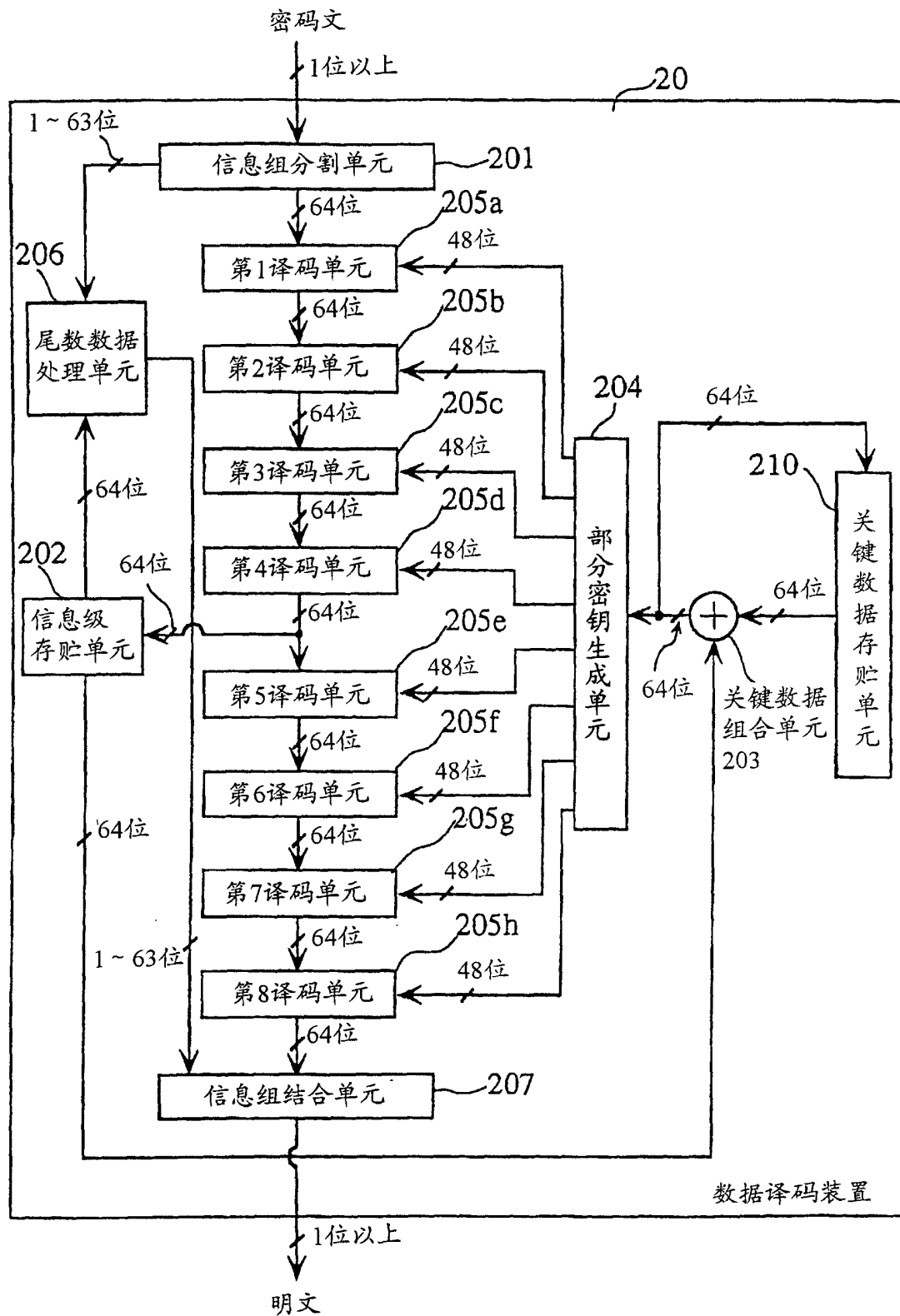


图 42

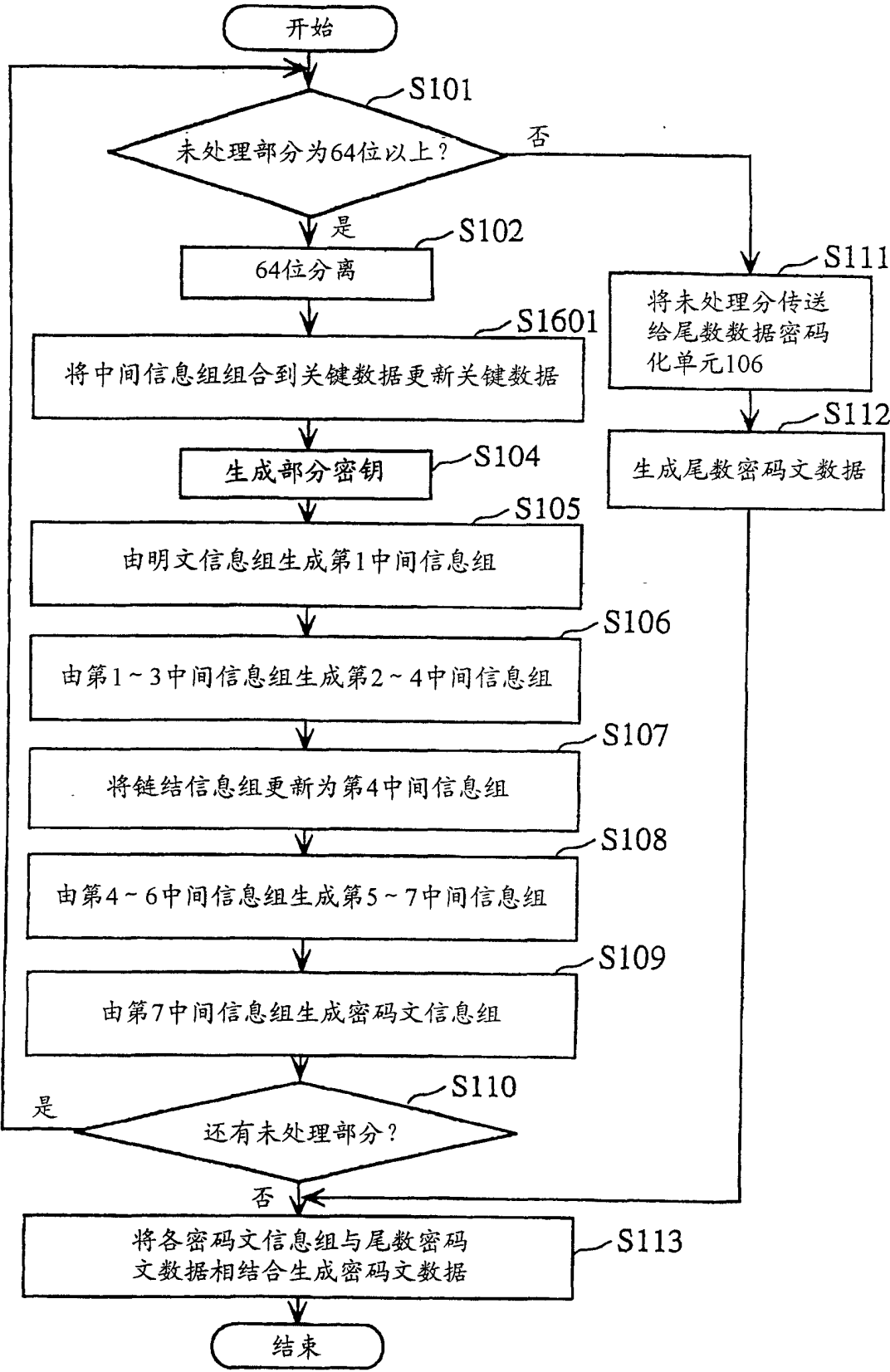


图 43

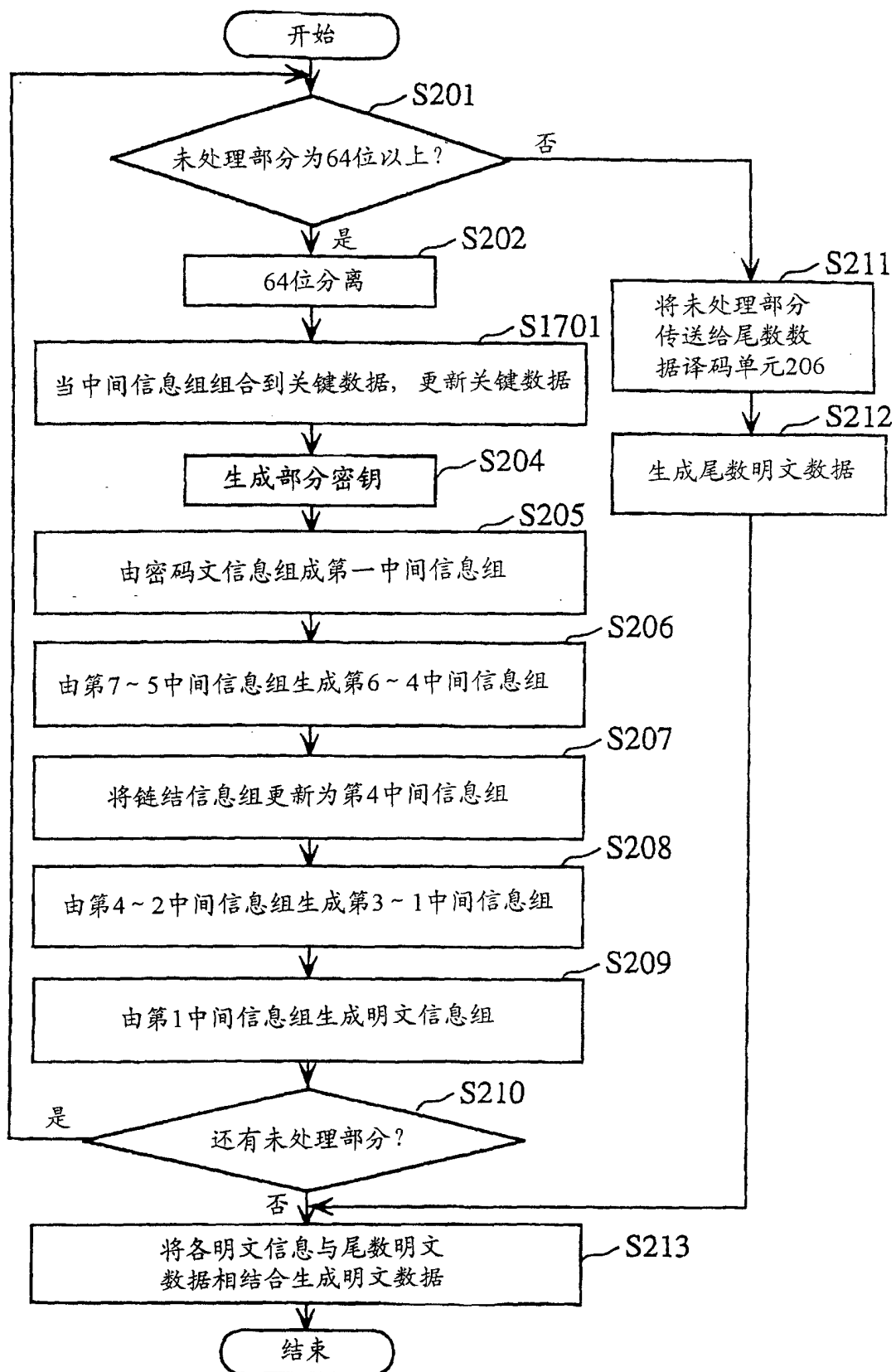


图 44

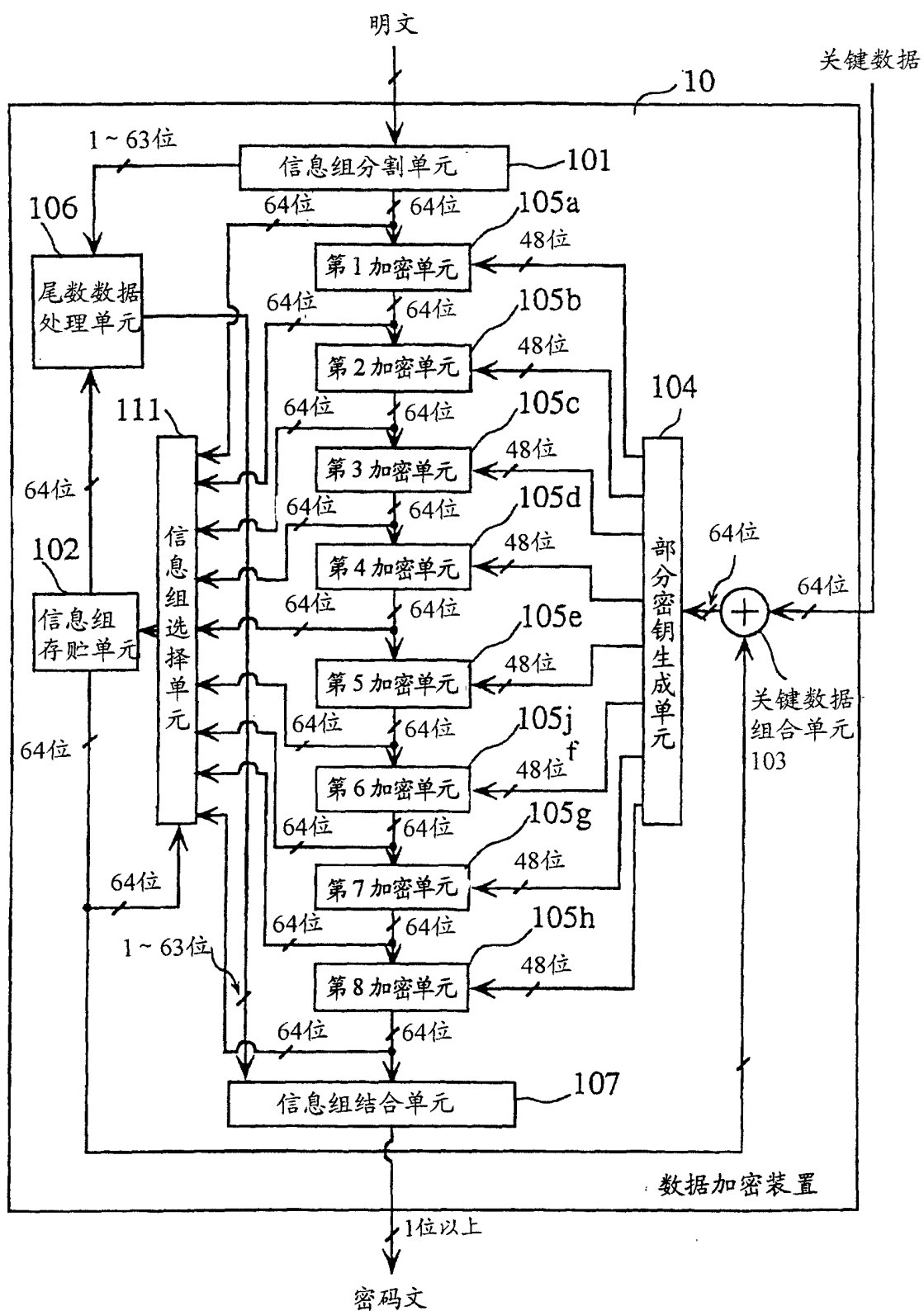


图 45

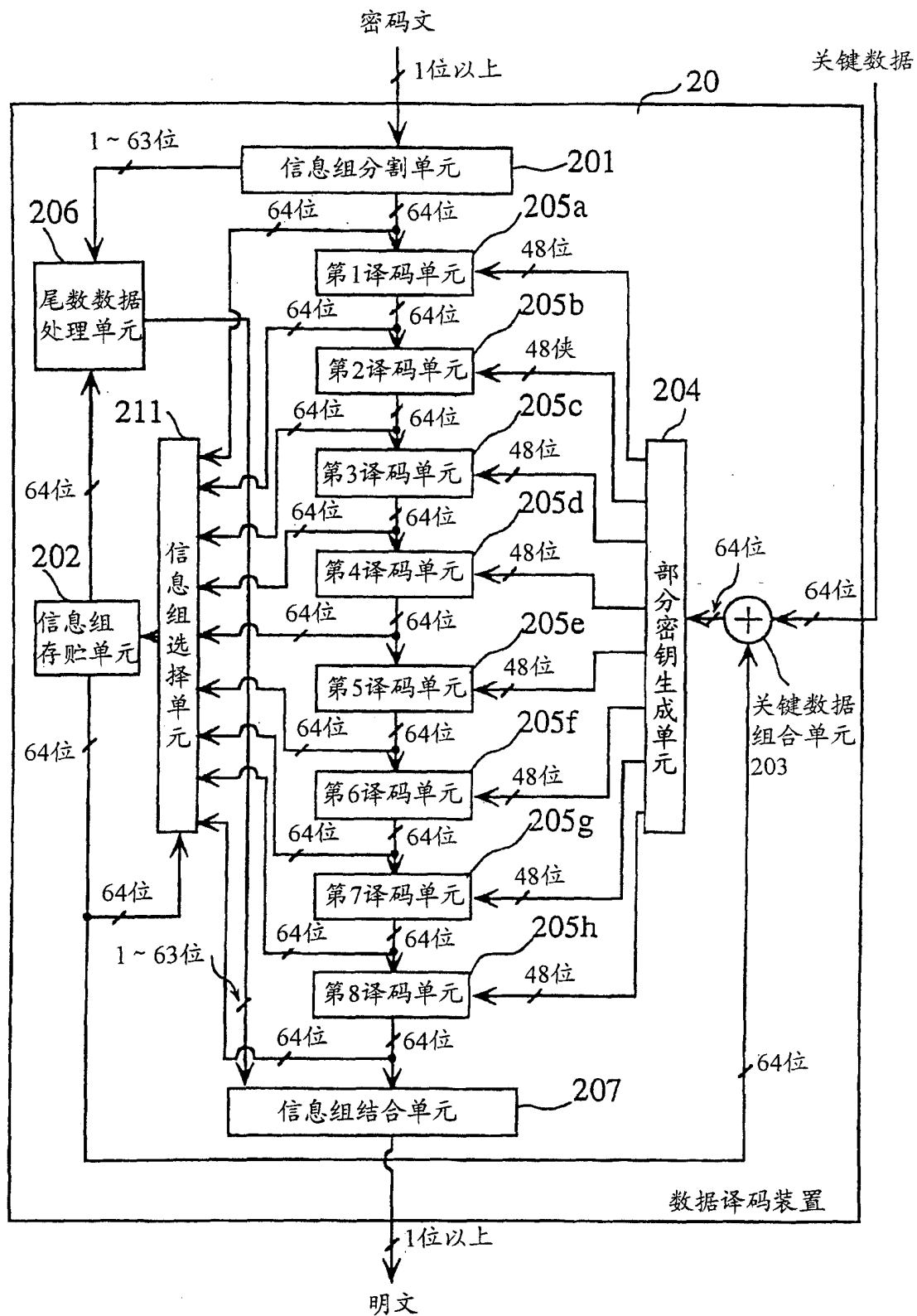


图 46

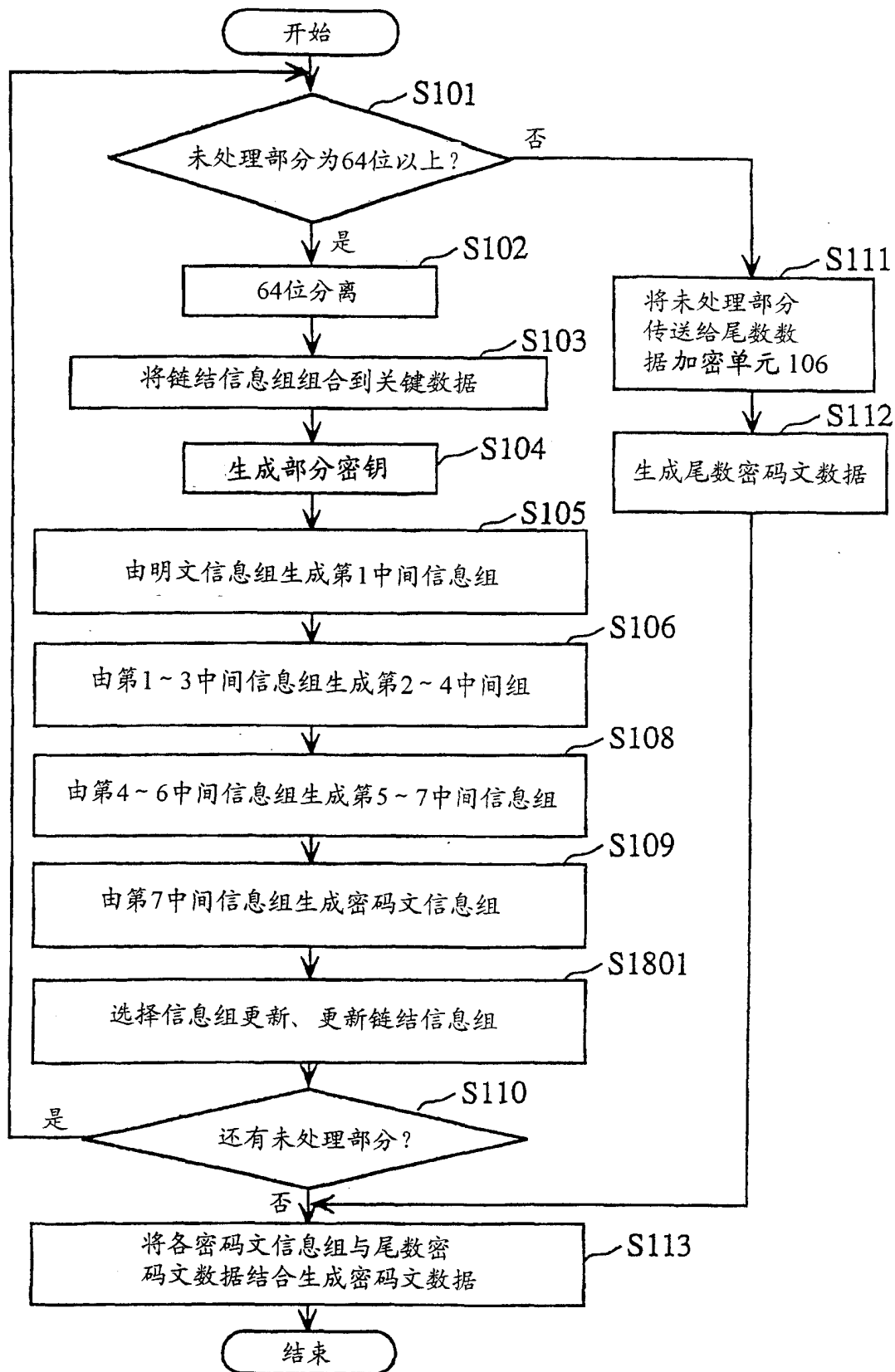


图 47

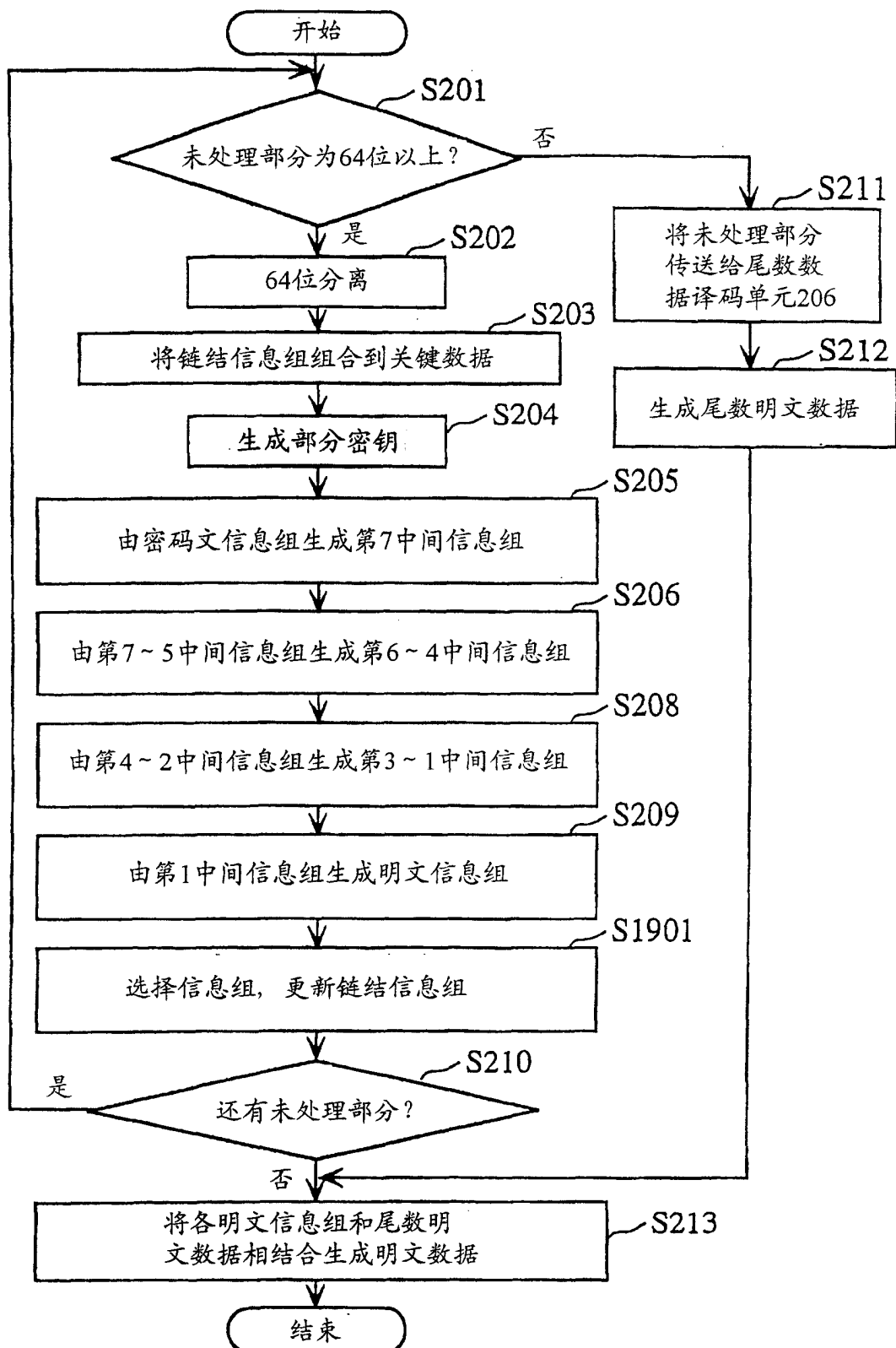


图 48

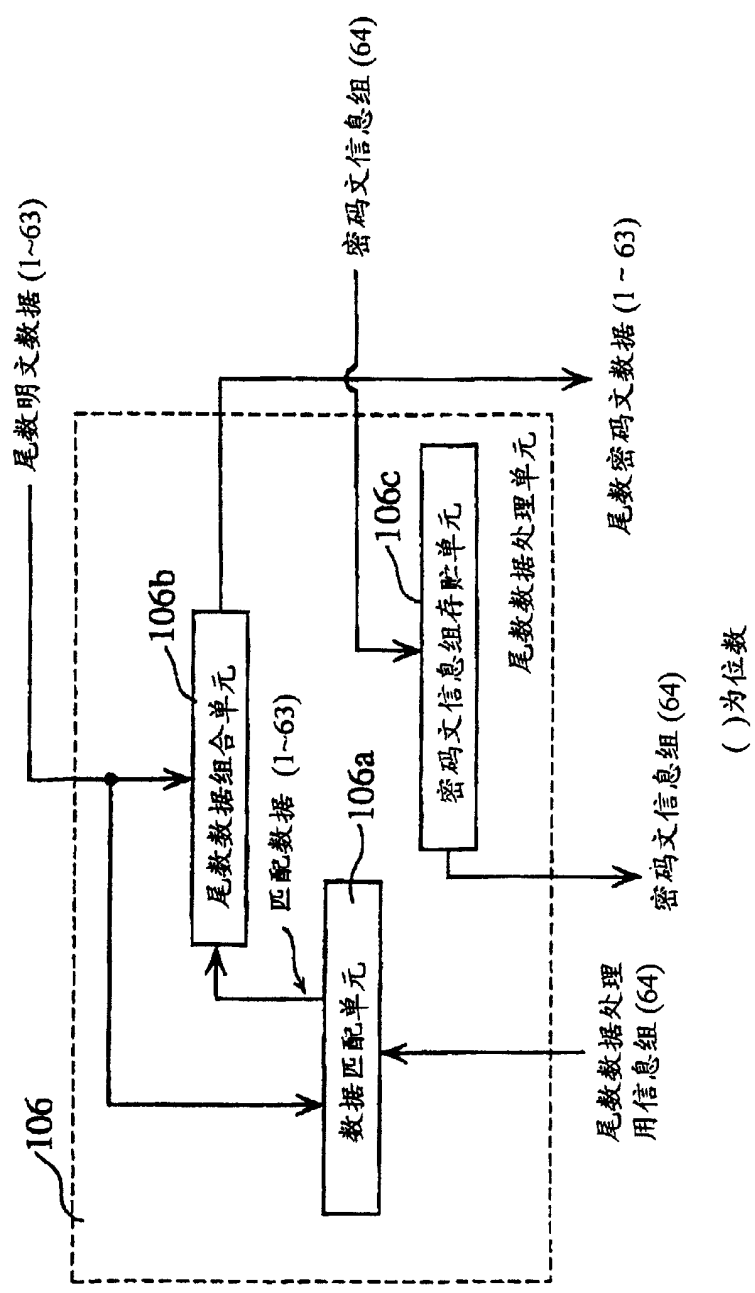


图 49

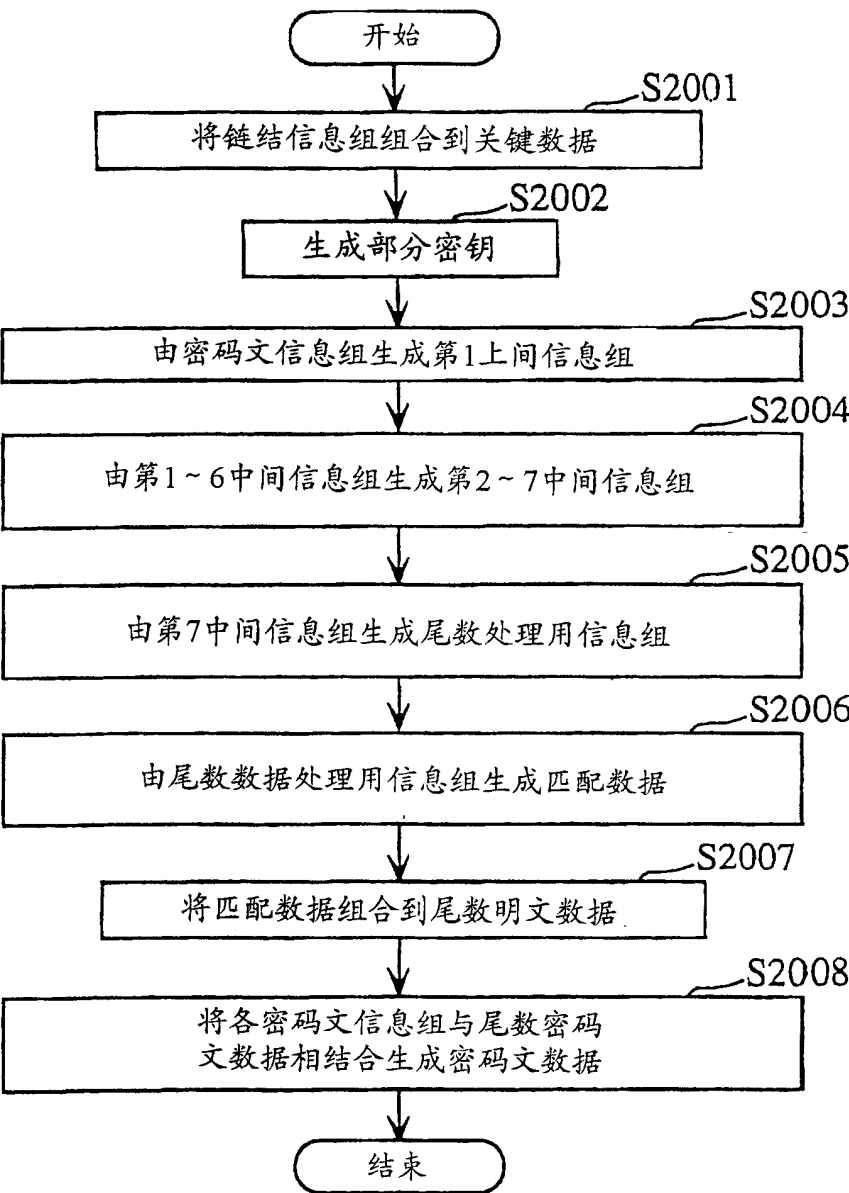


图 50