(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101060400 B
(45)授权公告日 2010.08.25

(21)申请号 200710093758.4

(22)申请日 2007.04.18

(30)优先权数据
2006-115013 2006.04.18 JP
2007-062483 2007.03.12 JP

(73)专利权人 佳能株式会社
地址 日本东京都大田区下丸子 3-30-2

(72)发明人 须贺祐治

(74)专利代理机构 北京林达刘知识产权代理事务所(普通合伙) 11277
代理人 刘新宇 权鲜枝

(51)Int.Cl.
H04L 9/30(2006.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)

(56)对比文件
US 5712914 A,1998.01.27, 全文.
CN 1136749 A,1996.11.27, 全文.
WO 03/084164 A1,2003.10.09, 全文.
CN 1579065 A,2005.02.09, 全文.

审查员 罗啸

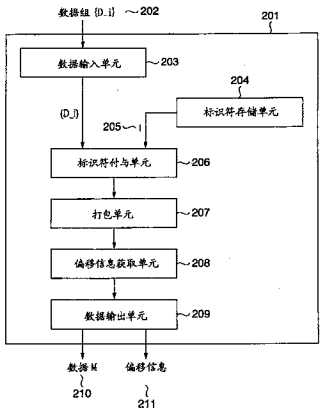
权利要求书 2 页 说明书 14 页 附图 9 页

(54)发明名称

数据生成装置、数据分析装置、控制方法和数据处理系统

(57)摘要

一种数据生成装置及其控制方法、数据分析装置及其控制方法、以及数据处理系统，该数据生成装置，包括：可变长度数据输入单元，用于输入可变长度数据；嵌入单元，用于将与表示可变长度数据的格式的格式信息相对应的识别数据嵌入到可变长度数据；位置信息获取单元，用于获取示出与可变长度数据中的识别数据相对应的位置的位置信息；以及输出单元，用于输出嵌入了识别数据的可变长度数据和位置信息；其中，可变长度数据包括公钥证书。



CN 101060400 B

1. 一种数据生成装置，包括：

可变长度数据输入单元，用于输入可变长度数据；

嵌入单元，用于将与表示所述可变长度数据的格式的格式信息相对应的识别数据嵌入到所述可变长度数据；

位置信息获取单元，用于获取示出可变长度数据中与识别数据相对应的位置的位置信息；以及

输出单元，用于输出嵌入了所述识别数据的所述可变长度数据和所述位置信息；

其中，所述可变长度数据包含构成公钥证书的信息。

2. 根据权利要求 1 所述的数据生成装置，其特征在于，还包括：

存储单元，用于相关联地存储识别数据和表示可变长度数据的格式的格式信息。

3. 根据权利要求 1 所述的数据生成装置，其特征在于，所述可变长度数据包括待验证的数据的哈希值和签名数据中的至少一个。

4. 根据权利要求 1 所述的数据生成装置，其特征在于，

所述公钥证书是 X.509 公钥证书；以及

所述识别数据被存储在 X.509 公钥证书的扩展项中。

5. 根据权利要求 1 所述的数据生成装置，其特征在于，还包括：

数据生成单元，用于以预定长度生成待由所述可变长度数据输入单元输入的至少一组数据。

6. 根据权利要求 5 所述的数据生成装置，其特征在于，

所述数据生成单元基于被签署数据和校正后的数据计算签名数据，如果所述签名数据的位长不是所述预定长度，则通过重复所述计算直到获得具有所述预定长度的签名数据为止来生成签名数据。

7. 根据权利要求 5 所述的数据生成装置，其特征在于，所述数据生成单元生成具有预定长度的公钥数据。

8. 一种数据分析装置，包括：

输入单元，用于输入待分析的数据，该数据为可变长度数据，并且包括识别数据；

存储单元，用于存储所述识别数据和与之相关联的表示该待分析的数据的格式的格式信息；

检测单元，用于检测所述待分析的数据中的所述识别数据；以及

分析单元，用于基于与所述识别数据相关联的所述格式信息来分析所述待分析的数据。

9. 根据权利要求 8 所述的数据分析装置，其特征在于，

所述输入单元还输入用于示出所述待分析的数据中与所述识别数据相对应的位置的位置信息；以及

所述检测单元基于所述位置信息进行所述检测。

10. 根据权利要求 9 所述的数据分析装置，其特征在于，

所述位置信息包括所述待分析的数据中与所述识别数据相对应的所述位置的起始位位置和数据长度中的至少一个。

11. 根据权利要求 8 所述的数据分析装置，其特征在于，所述待分析的数据是公钥证

书。

12. 根据权利要求 11 所述的数据分析装置，其特征在于，

所述公钥证书是 X.509 公钥证书；以及

所述识别数据被存储在所述 X.509 公钥证书的扩展项中。

13. 一种用于数据生成装置的控制方法，该控制方法包括以下步骤：

可变长度数据输入步骤，用于输入可变长度数据；

嵌入步骤，用于将与表示所输入的可变长度数据的格式的格式信息相对应的识别数据嵌入到所述可变长度数据；

位置信息获取步骤，用于获取表示所述可变长度数据中与所述识别数据相对应的位置的位置信息；以及

输出步骤，用于输出嵌入了所述识别数据的可变长度数据和所述位置信息；

其中，所述可变长度数据包含构成公钥证书的信息。

14. 一种用于数据分析装置的控制方法，该数据分析装置包括用于存储识别数据和与之相关联的表示待分析的数据的格式的格式信息的存储单元；该控制方法包括以下步骤：

输入步骤，用于输入待分析的数据，该数据为可变长度数据，且包括识别数据；

检测步骤，用于检测所述待分析数据中的识别数据；以及

分析步骤，用于基于与所述识别数据相关联的所述格式信息来分析所述待分析的数据。

15. 一种具有数据生成装置和数据分析装置的数据处理系统，

所述数据生成装置包括：

可变长度数据输入单元，用于输入可变长度数据；

嵌入单元，用于将与表示所述可变长度数据的格式的格式信息相对应的识别数据嵌入到所述可变长度数据；

位置信息获取单元，用于获取示出已嵌入了所述识别数据的可变长度数据中与识别数据相对应的位置的位置信息；以及

输出单元，用于输出嵌入了所述识别数据的可变长度数据和所述位置信息；

所述数据分析装置包括：

获取单元，用于获取嵌入了所述识别数据的可变长度数据，作为待分析的数据；

存储单元，用于相关联地存储识别数据和表示待分析的数据的格式的格式信息；

检测单元，用于检测所述待分析的数据中的所述识别数据；以及

分析单元，用于基于与所述识别数据相关联的所述格式信息，分析所述待分析的数据。

数据生成装置、数据分析装置、控制方法和数据处理系统

技术领域

[0001] 本发明涉及一种数据生成装置及其控制方法、数据分析装置及其控制方法、以及数据处理系统。特别地，本发明涉及一种用于有效分析可变长度数据的技术，尤其涉及一种用于有效分析公钥证书的技术。

背景技术

[0002] 在包括文本数据和图像数据的数字数据流过因特网等广域网时，由于数字数据易于被修改，因而存在第三方可能改变该数据的危险。考虑到该危险，已知一种被称为数字签名的技术，作为用于为了防止改变而认证数据，使得接受者可以检测所接收到的数据是否已经被改变的方法。数字签名技术还具有用于防止因特网上的电子欺骗和抵赖等功能，而不仅仅是防止数据改变。

[0003] 数字签名

[0004] 图 10 是示出签名创建处理和签名认证处理的示意图。参照该图给出数字签名技术的大体情况。在生成数字签名数据中使用哈希函数 (Hash function) 和公钥 (public key) 加密。在下文中，私钥 (private key) 为 Ks2106，而公钥为 Kp2111。

[0005] 当生成数字签名时，将哈希处理 2102 应用于输入的数据（消息）M2101，并且计算作为固定长度数据的摘要 H(M)(2103)。在哈希处理 2102 中使用以下所述的哈希函数。接着，使用私钥 Ks2106 将转换处理 2104 应用于该固定长度数据 H(M)，从而创建数字签名数据 S(2105)。数据的发送者在这些处理后，将数字签名数据 S(2105) 和输入数据 (M2101) 发送给接受者。

[0006] 在认证处理 2112 中，接受者首先利用公钥 Kp2111 对数字签名数据 S 应用转换（解密）处理 (2110)，并获取由此获得的数据。接着，认证该数据是否与通过对输入数据 M2107 应用哈希处理 2108 而获得的数据 2109 匹配。作为认证结果 (2113)，如果两组数据不匹配，则判断出数据 M 已经改变，而如果两组数据匹配，则判断出没有改变。因此，接受者可以检测有无改变。

[0007] 而且，数字签名方法包括已知的 RSA 和 DSA（以下详细说明）和基于公钥加密的其它方法。这些数字签名的安全性在于：对于私钥所有者之外的实体来说，用于伪造签名或破译私钥的计算复杂性所带来的困难程度。

[0008] 哈希函数 (Hash Functions)

[0009] 接着说明哈希函数。在数字签名方法中与数字签名处理一起使用哈希函数，以通过被签署数据 (signed data) 的不可逆压缩减少要计算的数据量，因而减少签名付与处理的时间量。哈希函数具有用于对具有任意长度的输入数据 M 施加处理并生成具有固定长度的输出数据 H(M) 的功能。在这种情况下，输出 H(M) 被称为纯文本数据 M 的哈希数据。

[0010] 特别地，单向哈希函数的特征在于：当接收数据 M 时，由于计算的复杂性，因而难以计算纯文本数据 M'，其中，H(M') = H(M)。作为这样的单向哈希函数已知有 MD2、MD5、SHA-1 和其它标准算法。

[0011] 公钥加密 (Public Key Encryption)

[0012] 接着说明公钥加密。公钥加密的特征是:使用两个相应的密钥,利用一个密钥加密的数据不可以利用另一密钥来解密。这两个密钥中的一个被称为公钥,对外界公开使用。另一密钥被称为私钥,保密该私钥,仅为所有者使用。

[0013] 作为公钥加密方法中所使用的数字签名已知有 RSA 签名、DSA 签名、Schnorr 签名和其它签名。作为例子说明 R.L.Rivest、A.Shamir 和 L.Adleman:“A Method for Acquiring DigitalSignatures and Public-Key Cryptosystems”,Communications ofthe ACM,v.21,n.2,pp.120-126,1978 年 2 月中所公开的 RSA 签名和 Federal Information Processing Standards(FIPS)186-2,Digital Signature Standard(DSS),2000 年 1 月中所公开的 DSA 签名。

[0014] RSA 签名

[0015] 生成素数 p 和 q 并令 n = pq。令 λ(n) 为 p-1 和 q-1 的最小公倍数。选择与 λ(n) 互质的适当元素 e,并令 d = 1/e(mod λ(n))。公钥为 e 和 n,而私钥为 d。令 H() 为哈希函数。

[0016] [创建 RSA 签名] 文档 M 的签名创建过程

[0017] 令 s := $H(M)^d \pmod n$ 为签名数据。

[0018] [验证 RSA 签名] 与文档 M 有关的签名 (s,T) 的验证过程

[0019] 验证 H(M) = $s^e \pmod n$ 是否为真。如果为真,那么判断出没有发生改变。如果不为真,那么判断出发生了改变。

[0020] DSA 签名

[0021] 令 p 和 q 为素数,且令 p-1 除尽 q。令 g 为从 Z_p^*(从阶为 p 的循环群 (cyclic group) Z_p 中省略 0 的乘法群 (multiplicative group)) 任意选择的阶为 q 的源(发生器)。令从 Z_p^* 任意选择的 x 为私钥,并令 y := $g^x \pmod p$ 为相应的公钥 y。令 H() 为哈希函数。

[0022] [创建 DSA 签名] 文档 M 的签名创建过程

[0023] 1) 从 Z_q 任意选择 α,并令 T := $(g^\alpha \bmod p) \bmod q$。

[0024] 2) 令 c := H(M)。

[0025] 3) 令 s := $\alpha^{-1}(c+xT) \bmod q$,且 (s,T) 为签名数据。

[0026] [验证 DSA 签名] 与文档 M 有关的签名 (s,T) 的验证过程

[0027] 验证 T = $(g^{h(M)s^{-1}} y^{Ts^{-1}} \bmod p) \bmod q$ 是否为真。如果为真,那么判断出没有发生改变。如果不为真,那么判断出发生了改变。

[0028] 公钥认证基本结构

[0029] 在客户机-服务器通信中,当客户机访问服务器资源时,通常需要用户认证。用户认证中所使用的众所周知的技术为 ITU-T Recommendation X.509 等公钥证书 (ITU-TRecommendation X.509/ISO/IEC 9594-8:“Informationtechnology-Open Systems Interconnection-The Directory:Public-key and attribute certificate frameworks”)。公钥证书是保证公钥与其用户相对应的数据,并且由被称为认证机构的可信赖的第三方对该数据应用数字签名。例如,基于验证用户是否具有与用户所呈现的公钥证书中所包含的公钥相对应的私钥来进行通过浏览器实现的使用 SSL(Secure Sockets Layer,安全套接层)的用户认证。

[0030] 通过从认证机构获得签名，对于有关公钥证书中所包含的用户和服务器的公钥的信息，可以信任公钥证书。换句话说，公钥证书中所包含的信息的可信任性是基于认证机构的数字签名的安全性。因为这个原因，如果在创建认证机构的签名中所使用的私钥被泄漏或变得脆弱，那么由该认证机构颁发的所有公钥证书将失去它们的可信任性，并变成无效。

[0031] 作为公钥证书的例子的 ITU-T Recommendation X.509 v.3 包含作为认证机构的被签署数据的认证实体（对象）的 ID 和公钥信息。通过对摘要使用例如上述 RSA 算法计算签名来生成认证机构的签名数据，其中，哈希函数已经应用于被签署数据。而且，被签署数据具有被称为扩展项 (extensions) 的可选字段，使得可以在应用程序或协议中包括唯一且新的扩展项数据。

[0032] X.509 v.3 格式

[0033] 图 11 是示出以 X.509 v.3 定义的公钥证书的典型格式的图。下面说明每一字段中所存储的信息。

[0034] 版本 2201 存储 X.509 的版本。该字段是可选的，并且如果省略，则表示 v1。序列号 (serialNumber)2202 存储认证机构唯一分配给该公钥证书的序列号。签名 2203 存储公钥证书的签名方法。颁发者 2204 存储作为公钥证书的颁发者的认证机构的 X.500 识别名称。有效性 2205 存储公钥的有效期（开始日期和时间、以及结束日期和时间）。对象 2206 存储与证书中所包含的公钥相对应的私钥的所有者的 X.500 识别名称。对象公钥信息 2207(subjectPublicKeyInfo) 存储被认证的公钥。

[0035] 颁发者唯一标识符 (issuerUniqueIdentifier)2208 和对象唯一标识符 (subjectUniqueIdentifier)2209 是 v2 中添加的可选字段。它们存储认证机构的唯一标识符和所有者的唯一标识符。

[0036] 扩展项字段 2210 是 v3 中添加的可选字段。它们包含由扩展项标识符 (extnID)2211、扩展项值 (extnValue)2213 和临界位 (critical)2212 构成的三部分组。v3 扩展项字段 2210 不仅可以包括 X.509 中提出的标准扩展项，而且还可以包括唯一且新的扩展项。因为这个原因，如何认证 v3 扩展项依赖于应用程序。而且，临界位 2212 表示是需要这些扩展项还是可以忽视这些扩展项。

[0037] 认证机构对构成上面的公钥证书的数据，使用认证机构的私钥生成签名 2214，并将签名 2214 付与公钥证书。公钥证书的用户可以使用签名 2214 验证公钥证书的合法性。

[0038] 公钥证书的分析

[0039] 使用上述数字签名技术具有防止因特网上的欺骗、数据改变、以及抵赖等的效果。设置了用于流通公钥证书的基本结构，作为可带来这种效果的可信赖的基本结构。近年来该可信赖基本结构被应用于更多种类的装置中，除 PC 和服务器以外，甚至在数字家用设备、便携式电话、以及 PDA 等中使用。因此，用于分析公钥证书所需的计算成本必须足够小，以使例如便携式终端能够计算它们。

[0040] 然而，用作公钥证书的事实上的标准格式的 X.509 公钥证书是以可变长度数据的一般描述方式 ASN.1 及其编码方法 DER(ISO/IEC 8825-1 :1995 Specification of Basic Encoding Rules(BER), Canonical Encoding Rules(CER), and DistinguishedEncoding Rules(DER)) 写的。因此，分析公钥证书的装置不仅必须执行用于解密计算的处理，而且还必须执行用于解析 (parsing)ASN.1 的处理，或者换句话说，分析作为可变长度数据的 DER

编码方法，这需要一定水平的计算成本。换句话说，为了使用 X.509 公钥证书所提供的可信赖基本结构，装置必须分析可变长度数据，这需要计算成本。

[0041] 根据这种状况，已知如下结构，其目的是允许在不解析 ASN.1 数据和其它类型的可变长度数据的情况下使用公钥基本结构。可以将这样的结构大体分成两种方法。

[0042] (1) 第一种方法是通过使用 SPKI(C.Ellison，SPKICertificate Theory，Request for Comments 2693，IETF，September1999) 等轻量公钥证书来减少验证处理中所涉及的计算成本的方法。当读取 SPKI 时，不必解析 ASN.1，并且也没有象 X.509 那样多的信息，这意味着可以在数字家庭设备和便携式电话等中利用少量 CPU 资源容易地使用该方法。

[0043] (2) 另一种方法是难以对 ASN.1 执行解析处理的装置将处理委托给作为代理进行签名验证、签名付与和其它处理的机构的方法。一个已知的例子是 XKMS(XML Key ManagementSpecification(XKMS 2.0)，http ://www.w3.org/TR/xkms2/，W3CCandidate Recommendation 5 April 2004)。

[0044] 然而，可以利用方法 (1) 认证的领域是有限的，并且与 X.509 不兼容。因此难以建立与因特网上已流行的认证基本结构的互操作性。

[0045] 而且，利用方法 (2)，必须以被信赖的方式进行机构（服务器）与装置之间的通信。这意味着 ：为了在服务器和装置之间进行安全通信，必须提供规定的认证方法等单独的机制。而且，为了使用 XKMS，还必须单独解析 XML。

[0046] 以上问题不局限于公钥证书的分析。换句话说，传统结构不能够低计算成本地分析使用现有可变长度数据格式描述的所有种类的可变长度数据，包括公钥证书。

发明内容

[0047] 考虑到这些问题设计了本发明，并且，本发明提供一种用于使得使用现有可变长度数据格式描述的可变长度数据的低计算成本分析成为可能的技术。

[0048] 为了实现此目的，本发明的一个方面提供了一种数据生成装置，该装置包括 ：

[0049] 可变长度数据输入单元，用于输入可变长度数据 ；

[0050] 嵌入单元，用于将与表示可变长度数据的格式的格式信息相对应的识别数据嵌入到可变长度数据 ；

[0051] 位置信息获取单元，用于获取示出可变长度数据中与识别数据相对应的位置的位置信息 ；以及

[0052] 输出单元，用于输出嵌入了识别数据的可变长度数据和位置信息 ；

[0053] 其中，可变长度数据包含公钥证书。

[0054] 本发明的另一方面提供了一种数据分析装置，该装置包括 ：

[0055] 输入单元，用于输入待分析的数据，该数据为可变长度数据，并且包括识别数据 ；

[0056] 存储单元，用于存储识别数据和与之相关联的表示该数据的格式的格式信息 ；

[0057] 检测单元，用于检测待分析的数据中识别数据 ；以及

[0058] 分析单元，用于基于与识别数据相关联的格式信息来分析待分析的数据。

[0059] 本发明的另一方面提供了一种用于数据生成装置的控制方法，该控制方法包括以下步骤 ：

[0060] 可变长度数据输入步骤，用于输入可变长度数据 ；

[0061] 嵌入步骤，用于将与表示输入的可变长度数据的格式的格式信息相对应的识别数据嵌入到可变长度数据；

[0062] 位置信息获取步骤，用于获取表示可变长度数据中与识别数据相对应的位置的位置信息；以及

[0063] 输出步骤，用于输出嵌入了识别数据的可变长度数据和位置信息；

[0064] 其中，可变长度数据包括构成公钥证书的信息。

[0065] 本发明的另一方面提供了一种用于数据分析装置的控制方法，该数据分析装置包括用于存储识别数据和表示该数据的格式的相关格式信息的存储单元，该控制方法包括以下步骤：

[0066] 输入步骤，用于输入待分析的数据，其中，该数据为可变长度数据，并包括识别数据；

[0067] 检测步骤，用于检测待分析的数据中的识别数据；以及

[0068] 分析步骤，用于基于与识别数据相关联的格式信息来分析待分析的数据。

[0069] 本发明的另一方面，提供了一种具有数据生成装置和数据分析装置的数据处理系统，其中，

[0070] 该数据生成装置包括：

[0071] 可变长度数据输入单元，用于输入可变长度数据；

[0072] 嵌入单元，用于将与表示可变长度数据的格式的格式信息相对应的识别数据嵌入到可变长度数据；

[0073] 位置信息获取单元，用于获取示出嵌入了识别数据的可变长度数据中与识别数据相对应的位置的位置信息；以及

[0074] 输出单元，用于输出嵌入了识别数据的可变长度数据和位置信息；

[0075] 该数据分析装置包括：

[0076] 获取单元，用于获取嵌入了识别数据的可变长度数据作为待分析的数据；

[0077] 存储单元，用于相关联地存储识别数据和表示数据格式的格式信息；

[0078] 检测单元，用于检测待分析的数据中的识别数据；以及

[0079] 分析单元，用于基于与识别数据相关联的格式信息，分析待分析的数据。

[0080] 通过以下（参照附图）对典型实施例的说明，本发明的其它特征显而易见。

附图说明

[0081] 图 1 是示出数据处理装置的硬件结构的框图。

[0082] 图 2 是示出生成可变长度数据中的功能结构的框图。

[0083] 图 3 是示出可变长度数据生成处理的流程的流程图。

[0084] 图 4 是示出可变长度数据分析装置的功能结构的框图。

[0085] 图 5 是示出可变长度数据分析处理的流程的流程图。

[0086] 图 6 是示出标识符检测单元的功能结构的框图。

[0087] 图 7 是示出数据分析单元所执行的数据分析处理的流程的流程图。

[0088] 图 8 是示出可变长度数据生成装置所执行的证书生成处理的流程的流程图。

[0089] 图 9 是示出用于生成具有规定长度的公钥的处理的流程的流程图。

[0090] 图 10 是示出签名创建处理和签名验证验证处理的示意图。

[0091] 图 11 是示出以 X.509 v.3 定义的公钥证书的典型格式的图。

具体实施方式

[0092] 以下参照附图详细说明本发明的实施例。然而，注意，这些实施例中所述的构成要素仅为示例性的，本发明的范围不局限于这些构成要素。

[0093] 第一实施例

[0094] 在该实施例中，存在用于生成可变长度数据的数据处理装置（以下称之为可变长度数据生成装置）和用于分析所生成的可变长度数据的数据处理装置（以下称之为可变长度数据分析装置）。可变长度数据生成装置和可变长度数据分析装置事先就正处理的可变长度数据的格式和标识符之间的对应关系取得一致。例如，事先共享关于可变长度数据中的某位位置中存储什么种类数据的信息（格式）和与其相对应的标识符。

[0095] 在这种状况下，可变长度数据生成装置输入可变长度数据，并将与输入的可变长度数据的格式相对应的标识符添加给可变长度数据。标识符用作表示可变长度数据可以作为相应格式的固定长度数据来分析的信息。

[0096] 同时，可变长度数据分析装置接受待分析的可变长度数据，并验证所接收的可变长度数据中是否包含标识符。如果包含标识符，那么可变长度数据分析装置判断出该数据以符合对应于标识符的格式的方式排列，使用与对固定长度数据所进行的处理相同的过程分析该可变长度数据，并进行规定处理。

[0097] 因此，利用根据本实施例的结构，如果在数据分析过程中成功检测到标识符，则可以在不解析可变长度数据情况下，以低成本分析可变长度数据。而且，根据目的和状况，可以在同一数据处理装置中实现可变长度数据生成装置和可变长度数据分析装置。

[0098] 图 1 是示出根据本实施例的数据处理装置的硬件结构的框图。例如，在个人计算机 (PC)、工作站 (WS) 或个人数字助理 (PDA) 等中实现根据本实施例的数据处理装置。而且，该数据处理装置不必包含本发明该实施例中图 1 所示的所有功能。

[0099] 数据处理装置的结构

[0100] 如图 1 所示，数据处理装置（主机）100 由通过总线 116 相互可通信连接的监视器 102、CPU 103、ROM 104、以及 RAM 105 等构成。

[0101] 在图 1 中，鼠标 112 和键盘 113 是用户向数据处理装置 100 输入命令等的操作单元。通过接口 111 将通过这些操作单元输入的信息（操作信息）读入数据处理装置 100。

[0102] 数据处理装置 100 中的各种类型的信息（字符信息、图像信息等）是可以通过打印机 115 打印的信息。打印机 115 通过接口 117 与数据处理装置 100 连接。

[0103] 作为显示单元的监视器 102 向用户显示命令信息、以及字符信息和图像信息等各种类型的信息。

[0104] CPU 103 管理数据处理装置 100 的整体操作控制，通过从硬盘 106 等读取并执行处理程序（软件程序）来控制整个数据处理装置 100。特别地，在本发明的实施例中，CPU 103 从硬盘 106 等将用于实现数据生成和分析的处理程序读入 RAM 105，并执行这些处理程序，从而应用下述信息处理。注意，读取程序的方面不局限于此，例如，可以通过使得从光盘、软盘、DVD 或其它介质直接将根据本实施例的程序和相关数据加载到 RAM105 并执行它们而构

成。可选地，还可以是如下结构，即，将由 CPU 103 直接执行的根据该实施例的程序记录在 ROM 104 中，以形成存储器映射的一部分。

[0105] ROM 104 是用于存储签名处理程序和这些程序中所使用的密钥数据等各种类型的数据的只读存储器。RAM 105 是可写存储器，例如，用作 CPU 103 中的为各种处理临时存储处理程序和待处理的信息的工作区。

[0106] 例如硬盘 106 等大容量存储装置保存各种类型的数据和例如在执行各种处理时传送给 RAM 105 的信息转换处理等处理程序。

[0107] CD(CD 驱动器)108 具有用于读取存储在作为外部存储介质的例子的 CD(CD-R) 上的数据的功能、以及用于将数据写到 CD 的功能。

[0108] 象 CD 108 一样，FD(软盘驱动器)109 读取存储在作为外部存储介质的例子的 FD(软盘)上的数据。FD 109 还具有用于将各种类型的数据写到 FD 的功能。

[0109] 象 CD 108 和 FD 109 一样，DVD(数字视频盘或数字多用途盘)110 是外部存储介质的例子。DVD 110 具有用于读取存储在 DVD 上的数据的功能和用于将数据写到 DVD 的功能。

[0110] 例如，在将用于编辑的程序或打印机驱动程序存储在 CD、FD 或 DVD 等外部存储介质上的情况下，可以是如下结构：将这些程序安装在硬盘 106 上，并在需要时将这些程序传送给 RAM105。

[0111] 接口 111 用于通过鼠标 112 或键盘 113 从用户接受输入。调制解调器 118 是经由接口 119、通过例如公共交换电话网与外部网络连接的通信调制解调器。网络连接单元 107 通过接口 114 与外部网络连接。

[0112] 而且，实施例还可以利用实现与以上装置相同功能的软件来取代这些硬件装置。

[0113] 为了便于说明，在该实施例中，说明了在单个装置中实现数据处理装置的结构，但是，还可以在将资源分布给多个装置的结构中实现本实施例。例如，可以以分布给多个装置的方式构成存储和计算资源。可选地，可以将资源分布给数据处理装置中虚拟实现的、进行并行处理的各个构成要素。

[0114] 可变长度数据生成处理

[0115] 接着，参照图 2 说明使用可变长度数据生成装置（进行可变长度数据生成处理的数据处理装置 100）的可变长度数据生成处理。图 2 是示出生成可变长度数据中的功能结构的框图。

[0116] 图 2 中所示的功能块执行由以上参照图 1 所述的数据处理装置的 CPU 103 加载到 RAM 105 中的程序，并通过与图 1 所示的硬件一起工作实现这些功能块。当然，可以利用专用硬件实现全部或部分功能块。

[0117] 可变长度数据生成装置 201 输入包含可变长度数据的数据组 {D_i}202，并生成包含表示该数据可作为固定长度数据来处理的信息（标识符）的可变长度数据 M210。

[0118] 在图 2 中，203 是用于输入数据组 {D_i}202 的数据输入单元 203。数据组 {D_i}202 是构成从可变长度数据生成装置 201 输出的可变长度数据 M210 的数据集合。例如，当利用可变长度数据生成装置 201 生成作为可变长度数据的公钥证书时，将包括公钥数据、公钥有效期、认证机构的识别数据等的信息集合输入数据输入单元 203，作为数据组 {D_i}202。

[0119] 可变长度数据生成装置 201 还配置有标识符存储单元 204、标识符付与单元 206、

打包单元 207、偏移信息获取单元 208、以及数据输出单元 209。标识符存储单元 204 使标识符 I205 与正处理的可变长度数据的格式有关的信息相关联，并将其存储和保存在规定的存储装置中。这里，标识符 I205 是表示可变长度数据生成装置 201 的输出 M210 可以基于相应格式的格式信息作为固定长度数据来处理并且可以构成为规定位串的信息。而且，关于格式的信息是如下信息：在可变长度数据的某位位置中存储什么数据，例如，可以由定义每一类型的数据的起始位位置的信息构成该信息。

[0120] 标识符付与单元 206 基于数据组 {D_i}202 生成可变长度数据，并将与所生成的可变长度数据的格式相对应的标识符 I205 添加给可变长度数据。打包单元 207 打包构成可变长度数据的数据组 {D_i}202 和标识符 I205。这里，打包处理是用于将多组数据组合成单组数据的处理，一个例子是 DER 编码。DER(Distinguished Encoding Rules，识别名编码规则）是用于将以用于定义数据结构的 ASN.1(Abstract Syntax NotationOne，抽象语法表示法 1) 语言定义的模板表示为二进制数据的方法。ASN.1 是 ISO 8824 下的标准，并可以分层描述一组｛数据类型，数据｝。通过进行 DER 编码，可以将包括｛数据类型，数据长度，数据｝的三部分组表示为单组二进制数据，这些是分层构成的，且可以以二进制格式唯一表示。DER 编码是基于 DER 规则的二进制转换的方法，并被用于因特网通信协议和数据格式。偏移信息获取单元 208 获取与可变长度数据 M210 中的标识符 I205 的位置有关的偏移信息（位置信息）作为输出数据。数据输出单元 209 输出作为来自可变长度数据生成装置 201 的输出结果（可变长度数据）的可变长度数据 M210、以及偏移信息 211。注意，这里给出了从数据输出单元 209 输出偏移信息 211 的例子，但是，可替代的，可以通过存储单元将偏移信息 211 存储在可变长度数据生成装置中。

[0121] 接着，参照图 3 说明可变长度数据生成装置 201 所执行的可变长度数据生成处理。图 3 是示出可变长度数据生成处理的流程的流程图。

[0122] 首先，在步骤 S301，输入构成可变长度数据的数据组 {D_i}202。

[0123] 在步骤 S302，判断在步骤 S301 输入的可变长度数据的格式，并从标识符存储单元 204 提取与该格式相对应的标识符 I205。

[0124] 接着，在步骤 S303，对在步骤 S302 中的构成可变长度数据的数据组 {D_i}202 和标识符 I205 进行打包处理。

[0125] 接着，在步骤 S304，获取与可变长度数据 M210 中的标识符 I205 的位置有关的偏移信息作为输出数据。例如，获取可变长度数据 M210 中的标识符 I205 的起始字节位置 n 和字节长度 m 作为偏移信息。在步骤 S305，输出可变长度数据 M210 和偏移信息。这里，给出了作为不同于可变长度数据 M210 的数据输出的偏移信息的例子，但是，偏移信息还可以是单独添加给可变长度数据 M210 的信息，或者是在可变长度数据生成装置或包括可变长度数据生成装置的系统中具有固定值的信息。

[0126] 如下所述，当包括标识符 I205 时，基于与标识符 I205 相对应的格式的格式信息，作为固定长度数据分析可变长度数据 M210。下面在对可变长度数据分析处理的说明中，详细给出了用于判断是否可以作为固定长度数据处理输出 M 的处理。

[0127] 可变长度数据分析处理

[0128] 接着，参照图 4 说明用于分析上述可变长度数据生成处理所生成的可变长度数据的可变长度数据分析处理。图 4 是示出可变长度数据分析装置的功能结构的框图。

[0129] 图 4 中所示的功能块是通过以上参照图 1 所述的数据处理装置的 CPU 103 加载到 RAM 105 中的程序，并且与图 1 中所示的硬件一起工作，通过执行这些程序实现这些功能块。当然，可以利用专用硬件实现全部或部分功能块。

[0130] 可变长度数据分析装置 401 输入可变长度数据 M402 和偏移信息，进行分析处理，并输出构成可变长度数据 M402 的数据组 {D_i}407。

[0131] 在图 4 中，403 是用于输入可变长度数据 M402 和偏移信息的数据输入单元。可变长度数据 M402 是通过上述可变长度数据生成处理所生成的数据。

[0132] 可变长度数据分析装置 401 还配置有标识符检测单元 404、数据分析单元 406、以及标识符存储单元 408。标识符检测单元 404 检测输入到数据输入单元 403 的可变长度数据 M 是否包括标识符 I405，如果包括，则获取标识符 I405。将所获取标识符 I405 传递给数据分析单元 406。数据分析单元 406 进行下述处理，并然后输出可变长度数据 M 中所包括的数据组 {D_i}407。象标识符存储单元 204 一样，标识符存储单元 408 使得标识符 I405 和与相应可变长度数据的格式有关的信息相关联，并将其存储和保存在规定的存储装置中。

[0133] 接着，参照图 5 说明可变长度数据分析处理。图 5 是示出可变长度数据分析处理的流程的流程图。

[0134] 首先，在步骤 S501，输入待分析的数据 M402。接着，在步骤 S502，进行用于从所输入的数据 M402 检测和获取标识符 I405 的处理。下面将详细说明该处理。接着，由于在步骤 S502 中检测到标识符 I405，因而在步骤 S503 中，判断出待分析的数据 M402 被排列成符合与检测到的标识符 I405 相对应的格式。换句话说，使用检测到的标识符 I405 作为搜索关键字来搜索标识符存储单元 408，并且提取与标识符 I405 相对应的格式信息。以与对具有所提取的格式的固定长度数据的处理相同的过程分析该可变长度数据。获取存储在数据 M402 中的数据组 {D_i}，并输出该数据组 {D_i} 作为输出结果。例如，如果待分析的可变长度数据 M402 为公钥证书，则获取并输出公钥数据、公钥的有效期、以及认证机构的识别数据等信息。然后完成可变长度数据分析处理。

[0135] 标识符检测处理

[0136] 以下参照图 6 说明标识符检测单元 404 检测标识符 I606 的处理的例子。图 6 是示出用于使用偏移信息 602 从可变长度数据 M603 检测标识符 I606 的标识符检测单元 404 的功能结构的框图。标识符检测单元 404 具有 ：偏移输入单元 604，用于输入通过待分析的数据 M603 中的标识符的位置所判断的偏移信息 ；以及标识符提取单元 605，用于输入待分析的数据 M603 和输出标识符 I606 作为输出结果。为了简化说明，以下假定偏移数据 602 为上述表示起始字节位置 n 和字节长度 m 的整数数据 n、m。

[0137] 标识符提取单元 605 在从待分析的数据 M603 的开头开始的第 n 个字节处开始读取 m 个字节（在偏移信息 602 中给出整数数据 n 和数据 m），并提取标识符 I。所提取的标识符 I606 被传递给数据分析单元 406，并基于标识符 I 的检测，对所提取的标识符 I606 进行固定长度数据分析处理。数据分析单元 406 的分析处理可以将该数据作为固定长度数据而不是作为可变长度数据来分析。

[0138] 如上所述，利用根据该实施例的结构，事先就作为固定长度数据处理的可变长度数据的格式达成一致，并且在分析可变长度数据时，如果可变长度数据中包括标识符，则基于与该标识符相对应的格式处理该数据。因此，可以作为固定长度数据分析可变长度数据，

从而降低了分析可变长度数据所需的计算成本，并使得可以进行有效分析。

[0139] 另外，在该实施例中，表示可变长度数据中标识符所占用的位置的偏移信息是标识符所占用的位置的起始位位置和数据长度，但是不局限于此。例如，可以仅使用起始位位置和数据中的一个，或者可以使用起始位位置和结束位位置。可选地，用以将分配给标识符的位置付与可变长度数据的开头或末端的结构，使得可以在不使用偏移信息的情况下检测有无标识符 I。

[0140] 第二实施例

[0141] 在第一实施例中，通过对可变长度数据分析装置的标识符检测单元设置使用数据偏移的标识符提取单元来检测待提取的标识符的位置。然而，如果没有给出符合待分析的数据的正确偏移信息，则可能出现不能进行正确的分析过程之后的分析的情况（不能处理），或者可能出现利用错误数据格式进行分析处理好像该数据是正确的情况（错误检测）。同样可能出现未将数据 M402 中所包含的标识符存储在标识符存储单元 408 中的情况。然而，如上所述，例如，偏移信息包含标识符 I 的可变长度数据中的起始位置 n 和数据长度 m 等。在该实施例中，对如下配置进行说明：即使在不能正确提取标识符 I 的情况下，也不会进行错误操作。而且，因为根据该实施例的配置大部分与第一实施例的相同，因而仅说明该实施例中不同的部分。

[0142] 以下参照图 7 说明图 4 的数据分析单元 406 中所执行的处理。图 7 是示出数据分析单元 406 所执行的数据分析处理的流程的流程图。

[0143] 首先，在步骤 S701，数据分析单元 406 输入标识符 I405，然后在步骤 S702，利用允许的标识符列表进行匹配处理，换句话说，判断在标识符存储单元 408 中所存储的标识符列表中是否存在输入的标识符 I405。如果在该标识符列表中存在标识符 I405（步骤 S 702 为“是”），则处理进入步骤 S703；如果不存在（步骤 S702 为“否”），那么处理进入步骤 S704。在步骤 S703，象在图 5 的步骤 S503 中一样，作为具有与输入的标识符 I405 相对应的格式的固定长度数据来分析该可变长度数据。另一方面，在步骤 S704，作为普通可变长度数据分析该可变长度数据，因为该可变长度数据不能作为固定长度数据来分析。

[0144] 给出对用以避免标识符 I 的错误检测的方法的补充说明。用于避免错误检测的一种方法是用于使得标识符足够长以充分降低错误检测的可能性的方法。例如，标识符为 4 字节长时的错误检测的可能性为 $(1/2)^{32}$。另外，有这样一种方法，该方法用于使标识符为存储的数据组 {D_i} 或数据类型，或者可选地，为不能作为标识符存储单元可获取的数据的字节串。例如，如果以 ASCII 码表示所存储的数据组，则通过使得标识符为 0xFFFFFFFF 可以防止错误检测。

[0145] 如上所述，该实施例的可变长度数据分析装置被构成为：如果不能从该数据检测到标识符 I，则作为普通可变长度数据分析输入数据 M402，如果检测到标识符 I，则可以作为固定长度数据快速分析该数据。

[0146] 而且，在根据该实施例的结构中，为了在数据分析过程中防止错误检测或不可能进行处理的情况，可以通过嵌入标识符来抑制分析处理发生中断或分析结果中出现问题。如果所提取的标识符 I 是不适当的，则检测和处理该标识符可以防止错误操作，即使没有正确提取标识符 I。

[0147] 第三实施例

[0148] 接着说明将根据本发明的该实施例应用于作为待分析的数据的公钥证书的情况的例子，具体来说是 X.509 公钥证书。X.509 公钥证书是 DER 编码的可变长度二进制数据，因此可容易应用于根据本发明的实施例。而且，因为本实施例与第一实施例大部分相同，因而仅说明本实施例中不同的部分。

[0149] X.509 公钥证书配置有被称为 X509v3 扩展项的可以存储应用程序或系统相关数据的区域（图 11 中的扩展项 2210）。因此，可以将标识符 I 存储在 v3 扩展项区域中。而且，对于可变长度数据分析装置分析作为固定长度数据的数据，需要参考 v3 扩展项区域，并且通过用固定长度表示除图 11 中的扩展项 2210 以外的区域，可变长度数据分析装置可以容易地参考标识符 I。

[0150] 以下参照图 2 和图 3 给出生成特定 X.509 公钥证书的例子。作为可变长度数据生成装置 201 的输入的数据组 {D_i}202 等同于以下图 11 中给出的信息。

[0151] - 版本 2201

[0152] - 序列号 2202

[0153] - 签名 2203

[0154] - 颁发者 2204

[0155] - 有效性 2205

[0156] - 对象 2206

[0157] - 对象公钥信息 2207

[0158] - 颁发者唯一标识符 2208

[0159] - 对象唯一标识符 2209

[0160] 在步骤 S301，可变长度数据生成装置输入这些可变长度数据。接着，在步骤 S302，对与输入的可变长度数据相对应的标识符 I205 进行用于将数据组 {D_i} 付与可变长度数据的处理。在步骤 S303，使用以 X.509 定义的 DER 编码从数据组 {D_i} 和标识符 I205 生成可变长度数据 M。换句话说，在步骤 S302 中，将事先与可变长度数据分析装置一致的格式相对应的标识符 I205 付与等同于图 11 中的扩展项 2210 的位置，并在步骤 S303 中进行 DER 编码。在步骤 S304，获取偏移信息，并在步骤 S305，以根据以 X.509 所定义的 DER 编码的格式输出 M 作为全部输出结果。这里，作为具体例子给出用于生成 X.509 公钥证书的例子，但是，生成处理和结构与第一实施例中的相同。

[0161] 在接收可变长度数据 M 时，可变长度数据分析装置提取标识符 I205，并基于与所提取的标识符 I205 相对应的格式，使用与第一实施例中相同的过程，即用于固定长度数据的处理，来分析可变长度数据 M。

[0162] 如上所述，利用该实施例的结构，可以作为固定长度数据来分析 X.509 公钥证书等数据。因此，可以在不解析可变长度数据的情况下，分析 X.509 公钥证书。因此，根据该实施例，可以提供如下技术，该技术能够容易地与因特网上已普遍的认证基本结构连接，并能够在不解析可变长度数据的情况下验证公钥证书。

[0163] 第四实施例

[0164] 在第三实施例中，生成 X.509 公钥证书，从而将扩展项以外的区域表示为固定长度。然而，构成 X.509 公钥证书的数据不仅仅是与颁发者或对象等计算结果无关地使位长维持恒定的信息。例如，存在其位长随着计算结果改变的信息，例如，认证机构对公钥证书

的签名 2214。当构成数据组 {D_i} 的数据的位长这样改变时，基于这类数据生成的可变长度数据的格式类型在数量上增加。因为这个原因，标识符存储单元 204 和 408 需要存储大量信息。

[0165] 在本实施例中，说明了可以通过生成符合规定格式的可变长度数据来减少在标识符存储单元 204 和 408 中存储的信息的量的结构。而且，因为本实施例与第一实施例大部分都相同，因而仅说明本实施例中不同的部分。

[0166] 图 8 是示出可变长度数据生成装置所执行的证书生成处理的流程的流程图。以下，作为位长根据计算结果而改变的信息的例子，说明数字签名数据，但是，本实施例中所述方法可以应用于其它类型的数据。

[0167] 首先，在步骤 S801，生成被签署数据。然而，该被签署数据包括下面所述的校正数据用的区域，并存储初始值（例如，0x0000）。例如，通过从存储装置获取待被签署的数据并添加校正数据用的区域来进行被签署数据的生成。

[0168] 接着，在步骤 S802 生成签名。可以将公知的方法应用于用于生成签名的处理。

[0169] 接着，在步骤 S803，判断在步骤 S802 所生成的签名数据的数据长度是否是预期长度，也就是说，符合存储在标识符存储单元 204 中的任一格式信息的长度。例如，可以通过准备用于存储符合该格式信息的签名数据的固定长度数据区域来进行该判断处理，如果最高有效字节为 0，则判断出该数据不是预期长度，而如果不是 0，则判断出该数据为预期长度。在步骤 S 803 的判断中，如果长度为预期长度（步骤 S803 为“是”），则结束处理，将签名数据与被签署数据进行组合，并且输出公钥证书。如果长度不是预期长度（步骤 S803 为“否”），那么处理进入步骤 S804。

[0170] 在步骤 S804，将上述校正数据（例如，通过加 1）更新成不同数据，并且再次进行步骤 S802 中的签名处理。可以象普通签名一样验证由此创建的签名数据，因此在用于验证签名的分析装置中不必包括特别机制。

[0171] 在 X.509 公钥证书中，可以使用扩展项 2210 作为校正用的区域。更具体地，可以将标识符 I 和校正数据一起存储在 X.509v3 扩展项中，例如，将标识符存储在 extnId 2211 中，而将校正数据存储在 extnValue 2213 中。

[0172] 如上所述，在本实施例中，进行反复试验类型的签名生成处理，在该处理中，更新校正数据，直到签名长度达到预期长度为止。这样，可以创建具有希望的数据长度的签名数据，从而作为结果，使得可以减少在标识符存储单元 204 和 408 中所存储的信息量。

[0173] 已经说明了用于使签名数据为固定长度的结构，但是可以使用类似方法为其它类型的信息获取具有希望的位长的数据。作为一个这样的例子，参照图 9 说明用于使公钥证书中所包括的公钥数据为固定长度的配置。

[0174] 图 9 是示出用于生成具有规定长度的公钥的处理的流程的流程图。在步骤 S901，进行密钥生成，在步骤 S902，检查作为密钥生成的结果的公钥数据的数据长度是否为预期长度。如果是预期长度（步骤 S902 为“是”），则结束处理，并输出密钥数据。如果作为步骤 S902 的检查结果，该数据不是预期长度（步骤 S902 为“否”），则在步骤 S901 中重新生成密钥。通过进行这种反复试验密钥生成处理，可以创建具有希望的数据长度的密钥数据。

[0175] 以上说明了用于在生成公钥证书时获取希望的长度的数据的例子，但是还可以对生成其它数据的情况执行用于获取希望的长度的数据的处理。进行该处理还可以减少在标

识符存储单元 204 和 408 中所存储的信息量。

[0176] 以上说明了用于为数据组 {D_i} 中的一个获取希望的长度的数据的例子，但是还可以为两个或更多个数据的情况获取希望的长度的数据。

[0177] 如果存在两种或更多种格式的可以生成的可变长度数据，那么可以配置成获取与这些格式中的一个相对应的数据。例如，可以进行下面的处理。假定由数据 d_1、d_2 和 d_3 构成数据组 {D_i} 的情况。在这种情况下，例如，生成第一数据 d_1，并且提取符合所生成的数据 d_1 的格式。如果不存在符合的格式，则重复生成数据 d_1，直到提取出符合的格式为止。接着，生成数据 d_2，并从第一提取的格式提取符合所生成的数据 d_2 的格式。如果不存在符合的格式，则重复生成数据 d_2，直到提取出符合的格式为止。接着，对数据 d_3 进行相似的生成处理。然后，执行可变长度数据生成处理，以将与符合所生成的数据 d_1、d_2 或 d_3 的格式相对应的标识符付与可变长度数据。利用该配置，如果存在两种或更多种格式的可以生成的可变长度数据，那么可以获取与这些格式中的一个相对应的数据。

[0178] 其它实施例

[0179] 在普通 X.509 公钥证书的验证处理中，将同一字母的大写和小写字符当作为相同文本进行该处理，如电子邮件地址。因此，由于不能通过对位进行简单比较来判断字符串的同一性，因而需要计算成本。相反，通过基于字节串的简单比较进行验证，将同一字母的大写和小写字符当作为不同文本来处理，可以进一步降低由验证所引起的计算成本。

[0180] 而且，作为公钥证书的签名方法，可以采用使用包括 RSA 签名的公钥加密方法的加密处理（保密）方法，而且还可以采用使用共同密钥加密方法的加密处理方法和 MAC(messageauthentication code，消息认证码）生成方法。换句话说，可以使用其它加密算法应用根据上述本实施例的结构。

[0181] 已经说明了本发明的实施例，但是，例如，本发明可以是系统、装置、方法、程序或存储介质等。例如，本发明可以用作由多个装置（例如，主机、接口装置、阅读器、打印机等）构成的系统的一部分，或者用作单个装置（例如，复印机、传真装置）的一部分。

[0182] 而且，根据本发明的实施例不局限于构成以上装置的元件或这些装置的组合。例如，这包括如下情况：通过直接或远程向系统或装置提供用于实现上述实施例的功能的程序，并且该系统或装置的计算机读取和执行所提供的程序代码，从而实现本发明。因此，为了在计算机本身上实现本发明的功能和处理而安装在计算机上的程序代码包括在本发明的技术范围中。换句话说，本发明包括用于实现本发明的功能和处理的任何计算程序。

[0183] 在这种情况下，程序代码本身实现这些实施例的功能。因此，本发明的技术范围包括程序代码本身和用于向计算机提供该程序代码的任何单元，或更具体地说，存储该程序代码的存储介质。

[0184] 作为用于存储这类程序代码的存储介质，例如，可以使用软盘、硬盘、光盘、磁光盘、CD-ROM、磁带、非易失性存储卡、ROM 等。

[0185] 本发明不局限于仅根据程序代码通过对装置进行控制来实现上述实施例的功能。例如，如果通过该程序代码与运行在计算机上的 OS（操作系统）或其它应用程序软件等一起实现这些实施例，那么，这些程序代码包括在本发明的技术范围中。

[0186] 而且，还可以在将从存储介质读取的程序写入插入计算机的功能扩展板或与计算机连接的功能扩展单元所配置的存储器后，通过程序命令实现上述实施例的功能。换句话

说，还可以通过功能扩展板或功能扩展单元所配置的 CPU 等进行全部或部分实际处理来实现上述实施例的功能。

[0187] 如上所述，利用本发明，可以提供一种能够对使用现有可变长度数据格式描述的可变长度数据进行低计算成本分析的技术。

[0188] 尽管参照典型实施例说明了本发明，但是应该理解，本发明不局限于所公开的典型实施例。所附权利要求的范围符合最宽的解释，以包含所有这类修改和等同结构和功能。

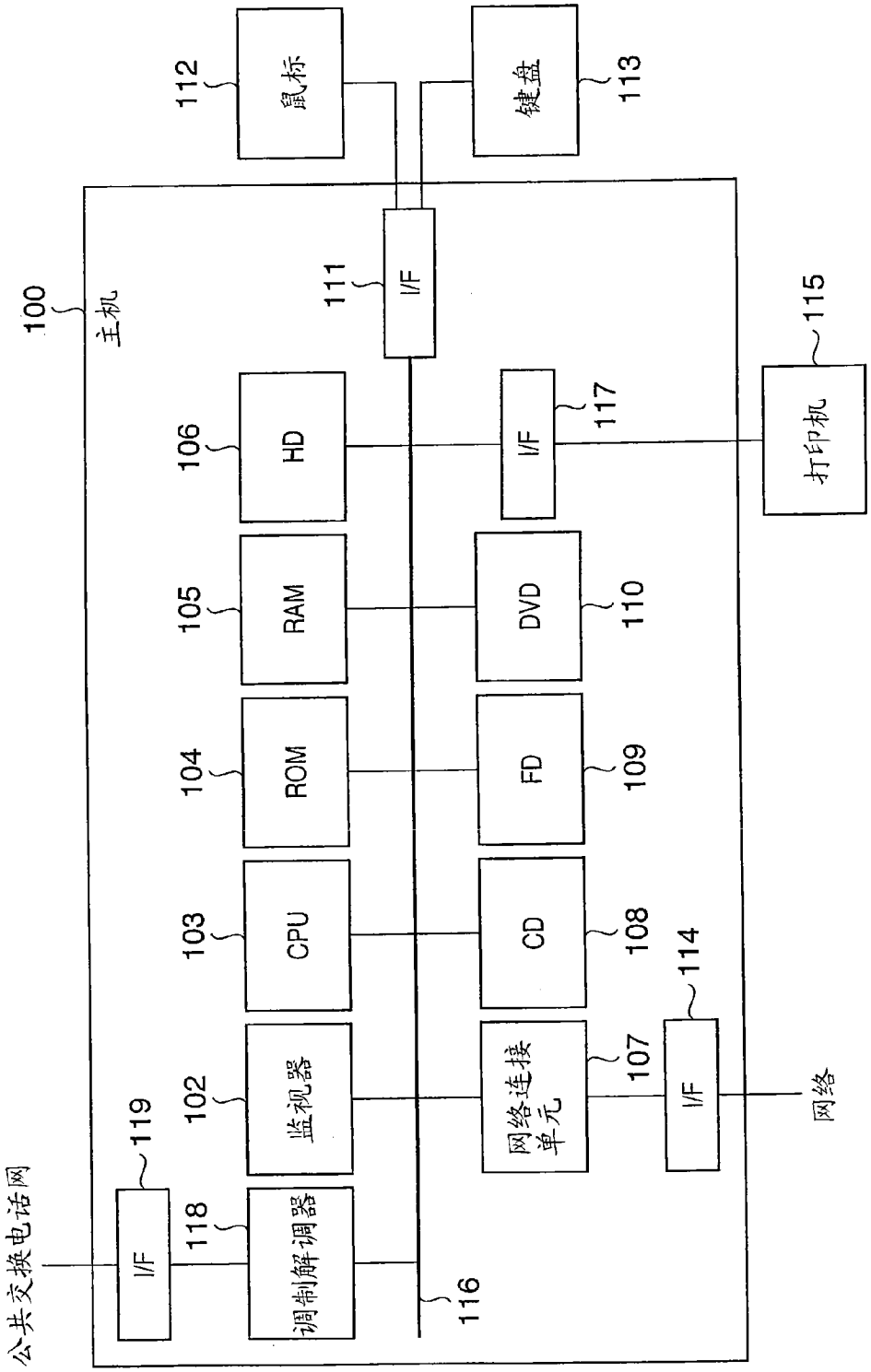

100
主机
111
I/F
112
鼠标
113
键盘
115
打印机
117
I/F
106
HD
105
RAM
110
DVD
104
ROM
109
FD
103
CPU
108
CD
114
I/F
107
网络连接单元
102
监视器
119
I/F
118
调制解调器
116
公共交换电话网
网络

图 1

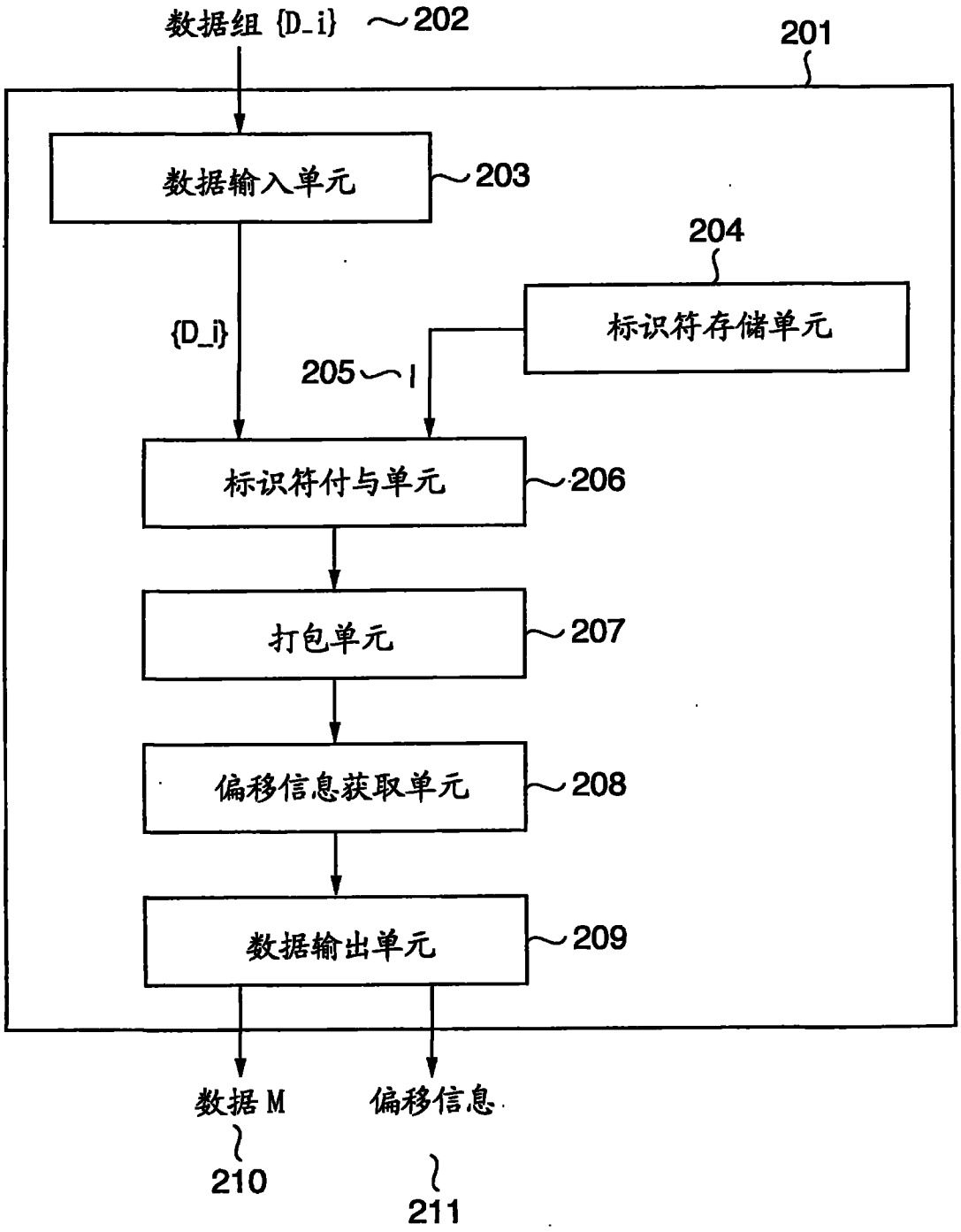

数据组 {D_i}
202
201
数据输入单元
203
204
标识符存储单元
{D_i}
205
标识符付与单元
206
打包单元
207
偏移信息获取单元
208
数据输出单元
209
数据 M
偏移信息
210
211

图 2

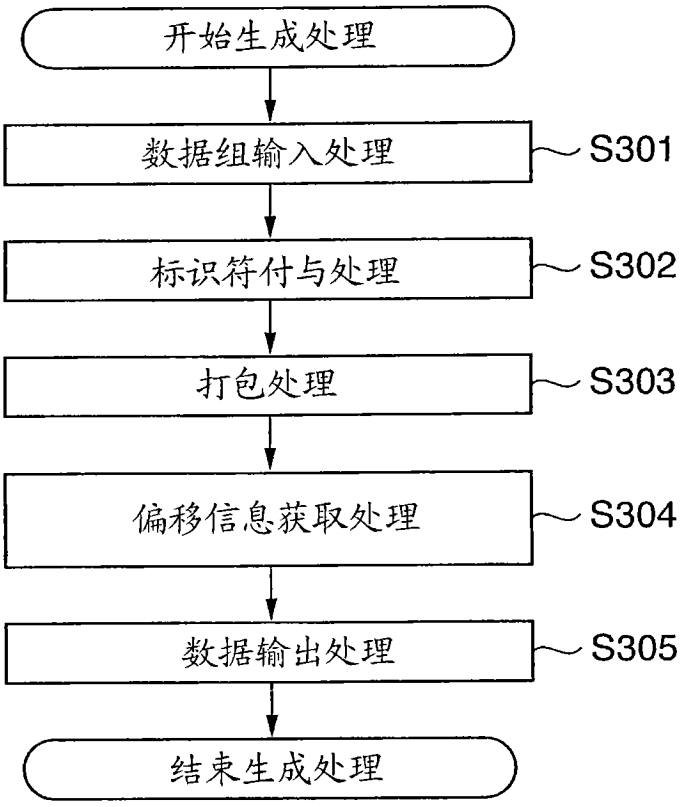

开始生成处理
数据组输入处理
S301
标识符付与处理
S302
打包处理
S303
偏移信息获取处理
S304
数据输出处理
S305
结束生成处理

图 3

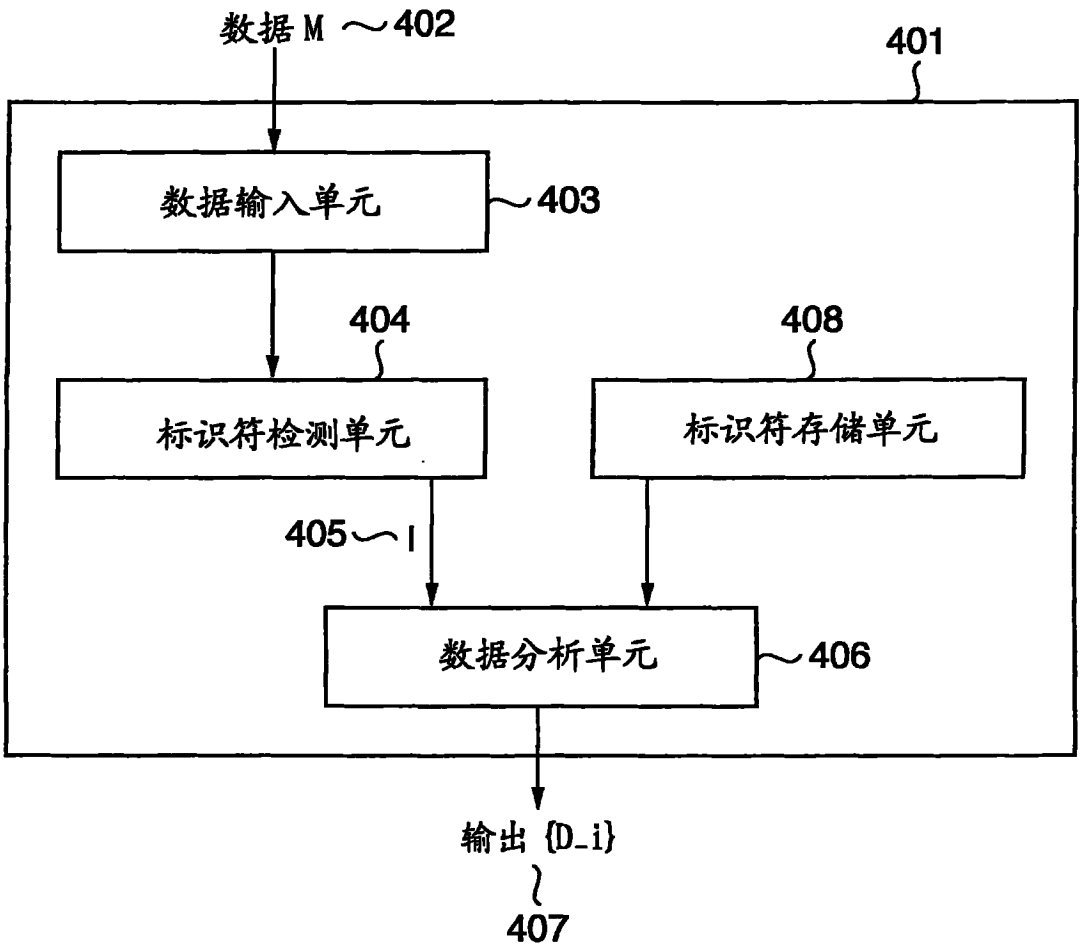

数据 M
402
401
数据输入单元
403
404
408
标识符检测单元
标识符存储单元
405
I
数据分析单元
406
输出 {D_i}
407

图 4

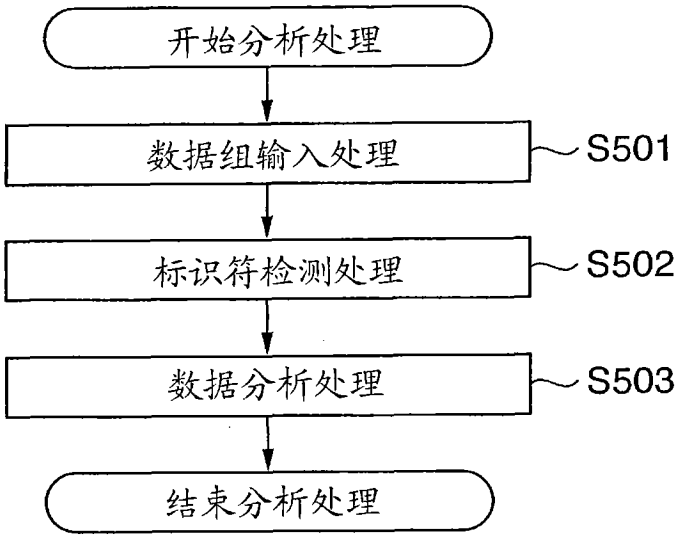

开始分析处理
数据组输入处理
S501
标识符检测处理
S502
数据分析处理
S503
结束分析处理

图 5

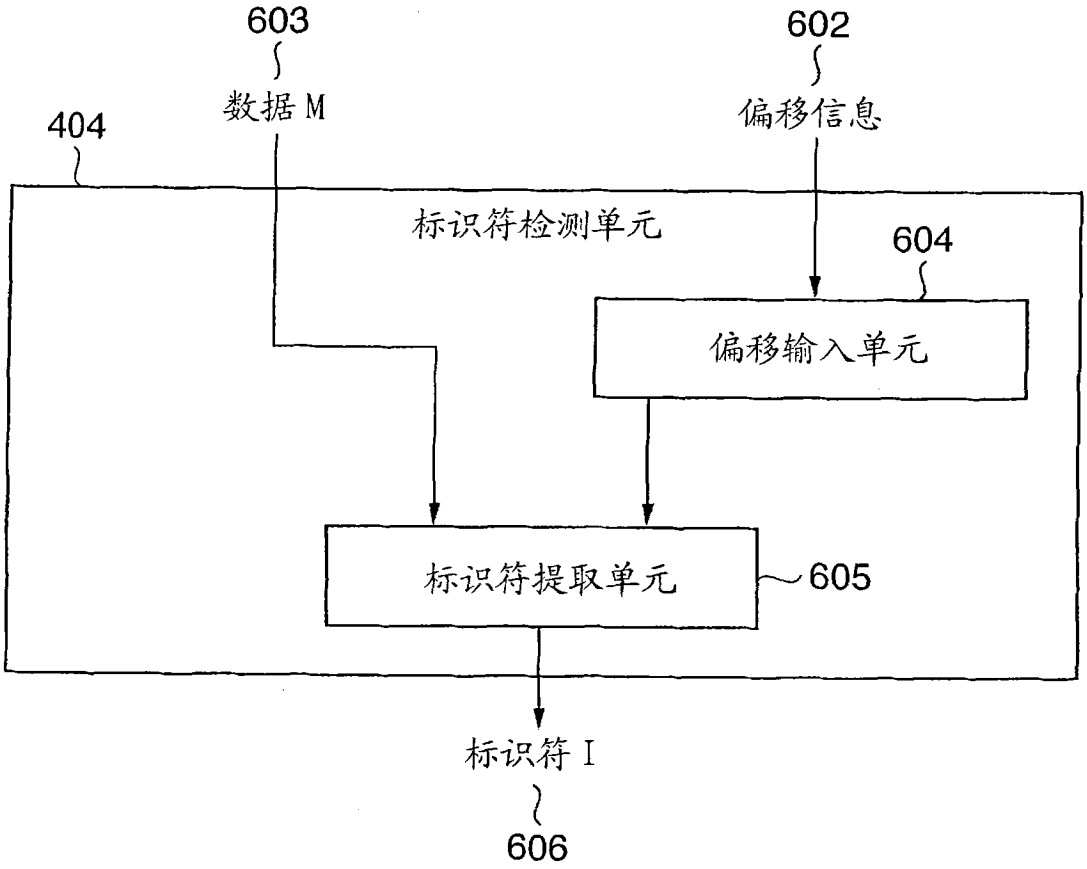


图 6

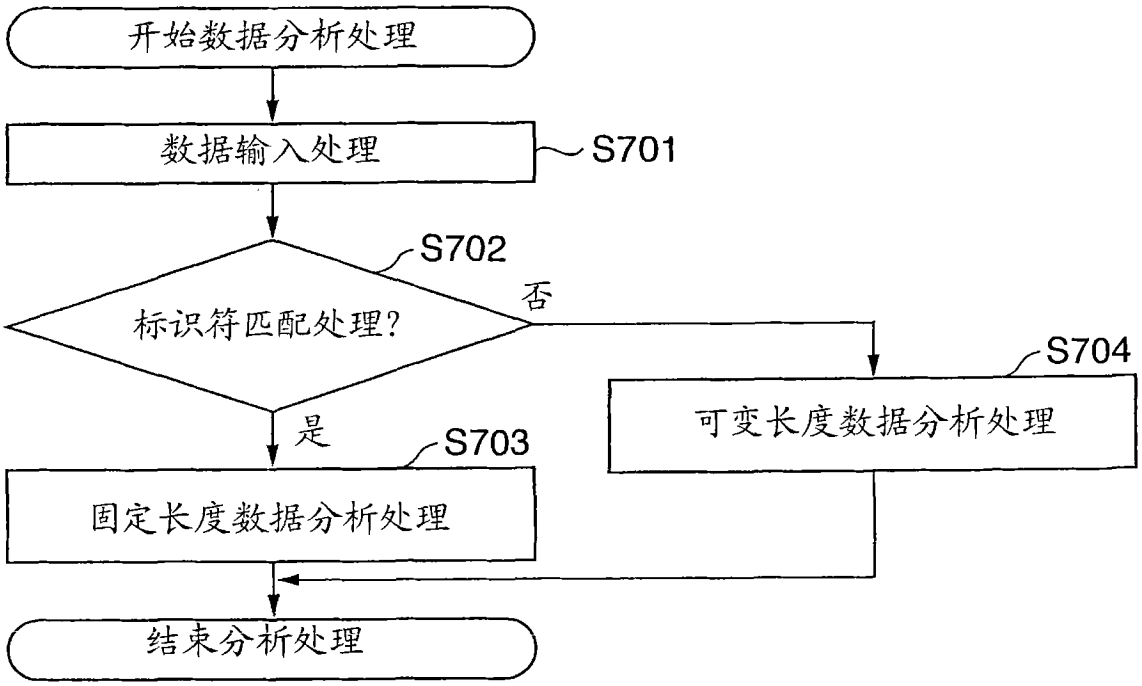

开始数据分析处理
数据输入处理
S701
S702
标识符匹配处理?
否
是
S703
固定长度数据分析处理
S704
可变长度数据分析处理
结束分析处理

图 7

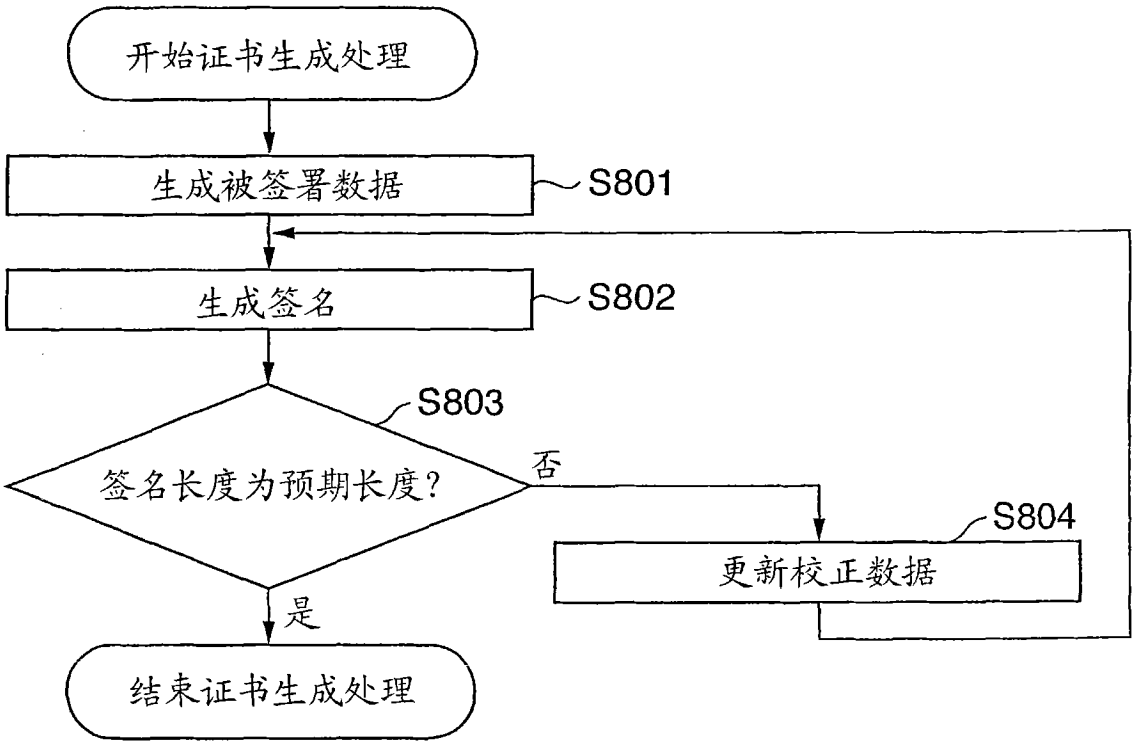

开始证书生成处理
生成被签署数据
S801
生成签名
S802
S803
签名长度为预期长度?
否
是
S804
更新校正数据
结束证书生成处理

图 8

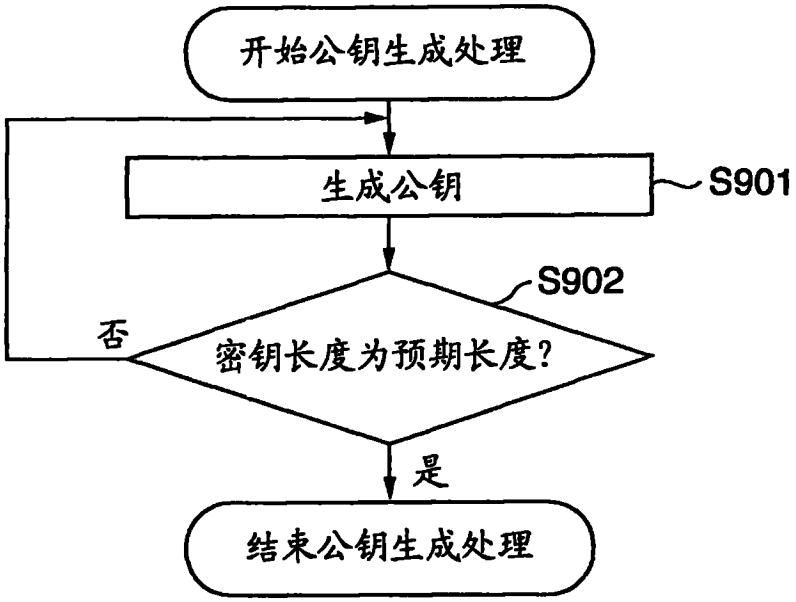


图 9

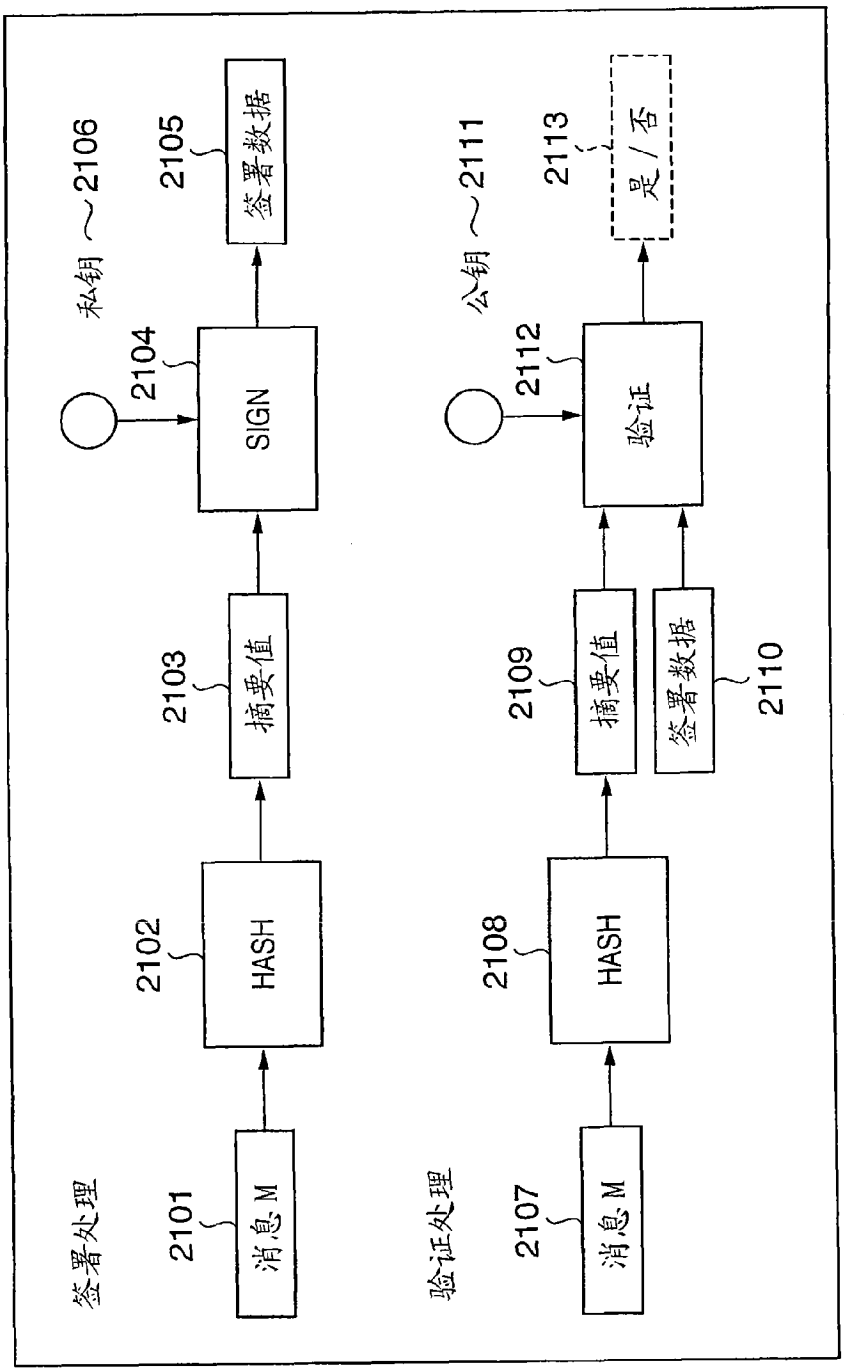

签署处理
2101
消息 M
2102
HASH
2103
摘要值
私钥
2104
SIGN
2105
签署数据
2106
验证处理
2107
消息 M
2108
HASH
2109
摘要值
2110
签署数据
公钥
2112
验证
2113
是 / 否
2111

图 10

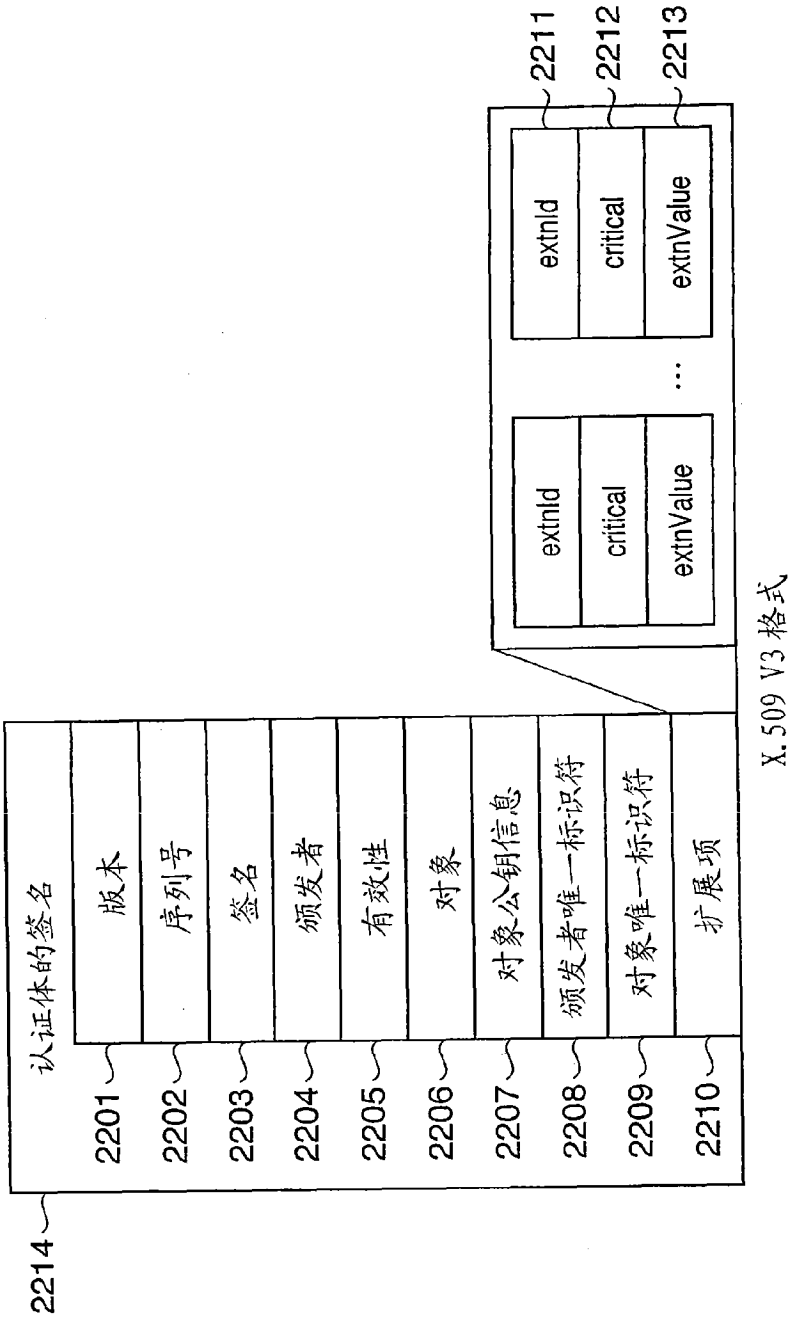

认证体的签名
版本
序列号
签名
颁发者
有效性
对象
对象公钥信息
颁发者唯一标识符
对象唯一标识符
扩展项
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
extnId
critical
extnValue
...
X.509 V3 格式

图 11