(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 103975553 B
(45)授权公告日 2016.10.12

(21)申请号 201180075191.2
(22)申请日 2011.11.30
(65)同一申请的已公布的文献号
申请公布号 CN 103975553 A
(43)申请公布日 2014.08.06
(85)PCT国际申请进入国家阶段日
2014.05.30
(86)PCT国际申请的申请数据
PCT/JP2011/077623 2011.11.30
(87)PCT国际申请的公布数据
WO2013/080320 JA 2013.06.06
(73)专利权人 三菱电机株式会社
地址 日本东京
(72)发明人 服部充洋 平野贵人 森拓海
伊藤隆 松田规
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 崔成哲
(51)Int.Cl.
H04L 9/30(2006.01)
G09C 1/00(2006.01)
(56)对比文件
CN 101057448 A,2007.10.17,
JP 2011211593 A,2011.10.20,
US 5991414 A,1999.11.23,
审查员 高伟

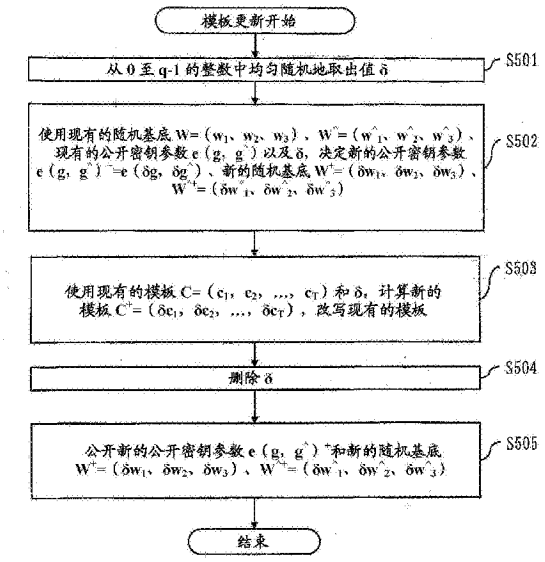
权利要求书2页 说明书23页 附图22页

(54)发明名称

数据处理装置以及数据处理方法

(57)摘要

存储部(301)将根据双重准同态密码算法生成的公开密钥、和使用该公开密钥加密了的数据存储为用于在认证中使用的模板。随机数生成部(203)使用存储部(301)内的公开密钥的至少一部分，生成随机数。模板更新部(307)进行使用了由随机数生成部(305)生成了的随机数的运算，更新模板。存储部(301)用更新了的模板盖写更新前的模板而存储。



CN 103975553 B

1.一种数据处理装置,其特征在于,具有:

公开密钥存储部,存储根据双重准同态密码算法生成的公开密钥;

加密数据存储部,将使用所述公开密钥加密了的第1数据存储为加密第1数据;

随机数生成部,使用所述公开密钥的至少一部分,生成随机数;

加密数据更新部,进行使用了由所述随机数生成部生成了的随机数的运算,更新所述加密第1数据;以及

公开密钥更新部,进行使用了由所述随机数生成部生成了的随机数的运算,更新所述公开密钥。

2.根据权利要求1所述的数据处理装置,其特征在于,

所述随机数生成部每当发生触发事件时,使用在触发事件发生时在所述公开密钥存储部中存储的公开密钥的至少一部分,生成随机数,

所述公开密钥更新部每当由所述随机数生成部生成随机数时,进行使用了由所述随机数生成部生成了的随机数的运算,更新在触发事件发生时在所述公开密钥存储部中存储的公开密钥,

所述加密数据更新部每当由所述随机数生成部生成随机数时,进行使用了由所述随机数生成部生成了的随机数的运算,更新在触发事件发生时在所述加密数据存储部中存储的加密第1数据,

所述公开密钥存储部每当由所述公开密钥更新部更新公开密钥时,用更新后的公开密钥盖写更新前的公开密钥而存储,

所述加密数据存储部每当由所述加密数据更新部更新加密第1数据时,用更新后的加密第1数据盖写更新前的加密第1数据而存储。

3.根据权利要求2所述的数据处理装置,其特征在于,

所述数据处理装置还具有公开密钥供给要求输入部,该公开密钥供给要求输入部从使用公开密钥对第2数据进行加密的密码装置,输入要求在所述第2数据的加密中使用的公开密钥的供给的公开密钥供给要求,

所述随机数生成部

在所述公开密钥供给要求输入部从所述密码装置输入了公开密钥供给要求时,判断为发生了所述触发事件,

每当所述公开密钥供给要求输入部从所述密码装置输入公开密钥供给要求时,使用在所述公开密钥存储部中存储的公开密钥的至少一部分,生成随机数,

所述公开密钥更新部每当由所述随机数生成部生成随机数时,进行使用了由所述随机数生成部生成了的随机数的运算,更新在所述公开密钥存储部中存储的公开密钥,

所述加密数据更新部每当由所述随机数生成部生成随机数时,进行使用了由所述随机数生成部生成了的随机数的运算,更新在所述加密数据存储部中存储的加密第1数据,

所述公开密钥供给要求输入部将由所述公开密钥更新部更新后的公开密钥作为所述密码装置中的所述第2数据的加密中使用的公开密钥,输出到所述密码装置。

4.根据权利要求3所述的数据处理装置,其特征在于,

所述数据处理装置还具有:

加密数据输入部,输入所述密码装置使用从所述公开密钥供给要求输入部输出了的更

新后的公开密钥对所述第2数据进行加密而生成了的加密第2数据;以及

加密类似度生成部,对在所述加密数据存储部中存储的加密第1数据和所述加密第2数据进行使用了在所述公开密钥存储部中存储的公开密钥的运算,生成在所述加密第1数据和所述加密第2数据分别被加密了的状态下、通过使用了与所述公开密钥对应起来的秘密密钥的解密处理能够导出所述第1数据与所述第2数据之间的类似度的加密了的信息,作为加密类似度信息。

5.根据权利要求4所述的数据处理装置,其特征在于,

所述加密数据存储部存储由通过所述密码装置对构成所述第1数据的T个部分数据进行加密而得到的T个加密了的部分数据构成的加密第1数据,其中T是2以上的整数,

所述加密数据输入部输入由通过所述密码装置对构成所述第2数据的T个部分数据进行加密而得到的T个加密了的部分数据构成的加密第2数据,其中T是2以上的整数,

所述加密类似度生成部针对每个部分数据,对所述加密第1数据和所述加密第2数据进行使用了在所述公开密钥存储部中存储的公开密钥的运算,生成能够导出所述第1数据的T个部分数据和所述第2数据的T个部分数据中的汉明距离的信息,作为所述第1数据与所述第2数据之间的类似度。

6.根据权利要求4所述的数据处理装置,其特征在于,

所述加密数据存储部存储由通过所述密码装置对构成所述第1数据的T个部分数据进行加密而得到的T个加密了的部分数据构成的加密第1数据,其中T是2以上的整数,

所述加密数据输入部输入由通过所述密码装置对构成所述第2数据的T个部分数据进行加密而得到的T个加密了的部分数据构成的加密第2数据,其中T是2以上的整数,

所述加密类似度生成部针对每个部分数据,对所述加密第1数据和所述加密第2数据进行使用了在所述公开密钥存储部中存储的公开密钥的运算,生成能够导出所述第1数据的T个部分数据和所述第2数据的T个部分数据中的欧几里得平方距离的信息,作为所述第1数据与所述第2数据之间的类似度。

7.根据权利要求1所述的数据处理装置,其特征在于,

所述加密数据更新部在更新了所述加密第1数据之后,删除在更新中使用了的随机数。

8.根据权利要求1所述的数据处理装置,其特征在于,

所述公开密钥存储部存储根据冈本-高岛密码算法生成了的公开密钥,作为根据所述双重准同态密码算法生成的公开密钥,

所述加密数据存储部存储通过利用根据所述冈本-高岛密码算法生成了的公开密钥的加密得到的加密第1数据。

9.一种数据处理方法,其特征在于,

计算机

存储根据双重准同态密码算法生成的公开密钥,

将使用所述公开密钥而加密了的第1数据存储为加密第1数据,

使用所述公开密钥的至少一部分,生成随机数,

进行使用了所生成了的随机数的运算,更新所述加密第1数据,

进行使用了所生成的随机数的运算,更新所述公开密钥。

数据处理装置以及数据处理方法

技术领域

[0001] 本发明涉及更新根据双重准同态密码算法生成并在认证中使用的加密数据(模板)的技术。

[0002] 此处,双重准同态密码(Doubly Homomorphic Encryption)是指,与通常的准同态密码不同,能够根据多个密文计算组合了原来的明文的有限体上的和及积的密文的密码,以使能够使用例如2T(T是2以上的整数)个密文$E(x_1)$、$E(x_2)$、...,$E(x_T)$、$E(y_1)$、$E(y_2)$、...、$E(y_T)$计算密文$E(x_1*y_1+x_2*y_2+...+x_T*y_T)$。

背景技术

[0003] 近年来,以大厦的出入管理、个人计算机的登录时的用户认证、银行ATM(Automated Teller Machine,自动取款机)中的本人认证等个人认证为目的,使用了指纹认证、静脉认证等生物体认证。

[0004] 一般,如以下那样,进行生物体认证。

[0005] 首先,用户预先将自己的生物体信息作为模板登记到验证者侧。

[0006] 然后,在认证时,用户将自己的生物体信息作为认证信息对验证者提示,验证者将其与模板进行核对。

[0007] 如果模板和认证信息类似,则判定为本人,如果不类似,则判定为他人。

[0008] 在生物体认证中利用的生物体信息中,有指纹信息、静脉信息、虹膜信息、掌纹信息、DNA(Deoxyribonucleic acid,脱氧核糖核酸)信息等种类,但它们被考虑为隐私信息,本来不优选将这些信息对验证者侧公开。

[0009] 因此,作为用于对这些信息进行隐匿的同时认证个人的技术,以本申请申请人公开了的专利文献1为首,考虑了几个隐匿核对技术(例如专利文献1、专利文献2、非专利文献1)。

[0010] 即,在这些隐匿核对技术中,用户对验证者登记加密了的模板,并且在认证时,用户对验证者提示加密了的生物体信息,验证者核对加密了的模板和加密了的生物体信息。

[0011] 另外,作为能够在模板以及生物体信息的加密中利用的双重准同态密码算法,例如,有非专利文献2-5公开的密码算法。

[0012] 【专利文献1】国际公开WO11/052056号公报

[0013] 【专利文献2】日本特开2007-293807号公报

[0014] 【非专利文献1】Takato Hirano,Takumi Mori,Mitsuhiro Hattori,Takashi Ito,and Nori Matsuda,"Homomorphic encryption based countermeasure against active attacks in privacy-preserving biometric authentication,"IEICE Transactions,ISEC2010-73,pp.7-14,2011.

[0015] 【非专利文献2】T.Okamoto and K.Takashima,"Homomorphic encryption and signatures from vector decomposition,"Pairing2008,Lecture Notes in Computer Science volume5209,pp.57-74,2008.

[0016] 【非专利文献3】D.Boneh,E.-J.Goh,and K.Nissim,“Evaluating2-DNF formulas on ciphertexts,”Theory of Cryptography Conference,Lecture Notes in Computer Science,volume3378,pp.325-341,2005.

[0017] 【非专利文献4】C.Gentry,“Fully homomorphic encryption using ideal lattices,”ACM Symposium on theory of computing,pp.169-178,2009.

[0018] 【非专利文献5】D.Freeman、M.Scott、E.Teske、“A taxonomy of pairing-friendly elliptic curves”、Journal Of Cryptology、2009年6月.

发明内容

[0019] 在专利文献1中,本申请申请人公开了将利用特征矢量的核对方式作为对象,使用冈本-高岛准同态密码(非专利文献2)、BGN(Boneh-Goh-Nissim)密码(非专利文献3)等双重准同态密码来实现隐匿核对的方法。

[0020] 为了预防在验证者侧保存的加密模板泄漏了的情况,需要安全地更新加密模板,但在专利文献1中,未公开加密模板的更新的方法。

[0021] 另外,在非专利文献1中,公开了同样地将利用特征矢量的核对方式作为对象,使用冈本-高岛准同态密码、BGN密码等双重准同态密码来实现隐匿核对,进而导入应用了征询-应答的考虑方法的手法,从而防止重放攻击的方法。

[0022] 但是,尚未公开用于安全地更新模板的方法。

[0023] 另一方面,在专利文献2中,针对利用图像的核对方式,公开了用于安全地更新模板的方法。

[0024] 但是,信息的隐匿方法特化为图像,所以存在仅能够应用于利用图像的核对方式这样的课题。

[0025] 本发明是鉴于这些点而完成的,其主要目的在于安全地更新根据双重准同态密码算法生成并在认证中使用的加密数据(模板)。

[0026] 本发明提供一种数据处理装置,其特征在于,具有:

[0027] 公开密钥存储部,存储根据双重准同态密码算法生成的公开密钥;

[0028] 加密数据存储部,将使用所述公开密钥加密了的第1数据存储为加密第1数据;

[0029] 随机数生成部,使用所述公开密钥的至少一部分,生成随机数;以及

[0030] 加密数据更新部,进行使用了由所述随机数生成部生成了的随机数的运算,更新所述加密第1数据。

[0031] 根据本发明,能够更新加密数据,所以即使在加密数据泄漏了的情况下,也能够有效地对抗使用了泄漏了的加密数据的“冒充”,能够提高保密强度。

附图说明

[0032] 图1是示出实施方式1的生物体认证系统的结构例的图。

[0033] 图2是示出实施方式1的证明装置的结构例的图。

[0034] 图3是示出实施方式1的认证装置的结构例的图。

[0035] 图4是示出实施方式1的解密装置的结构例的图。

[0036] 图5是示出实施方式1的模板更新处理的例子的流程图。

[0037] 图6是示出实施方式2的模板更新处理的例子的流程图。

[0038] 图7是示出实施方式3的重放攻击对策的例子的流程图。

[0039] 图8是示出实施方式4的重放攻击对策的例子的流程图。

[0040] 图9是示出实施方式5的设置处理的例子的流程图。

[0041] 图10是示出实施方式5的生物体信息的登记处理的例子的流程图。

[0042] 图11是示出实施方式5的认证处理的例子的流程图。

[0043] 图12是示出实施方式5的认证处理的例子的流程图。

[0044] 图13是示出实施方式5的认证处理的例子的流程图。

[0045] 图14是示出实施方式6的设置处理的例子的流程图。

[0046] 图15是示出实施方式6的生物体信息的登记处理的例子的流程图。

[0047] 图16是示出实施方式6的认证处理的例子的流程图。

[0048] 图17是示出实施方式6的认证处理的例子的流程图。

[0049] 图18是示出实施方式6的认证处理的例子的流程图。

[0050] 图19是示出实施方式5以及6的设置处理的概要的流程图。

[0051] 图20是示出实施方式5以及6的生物体信息的登记处理的概要的流程图。

[0052] 图21是示出实施方式5以及6的认证处理的概要的流程图。

[0053] 图22是示出实施方式5以及6的认证处理的概要的流程图。

[0054] 图23是示出实施方式1-6的证明装置、认证装置、解密装置的硬件结构例的图。

[0055] 符号说明

[0056] 101：证明装置；102：认证装置；103：解密装置；201：生物体信息抽出部；202：特征矢量形成部；203：随机数生成部；204：加密部；205：存储部；206：通信部；301：存储部；302：加密类似度生成部；303：判定部；304：通信部；305：随机数生成部；306：公开密钥更新部；307：模板更新部；401：参数生成部；402：解密部；403：存储部；404：通信部。

具体实施方式

[0057] 在本说明书中，关于利用特征矢量的核对方式，公开安全地更新模板的方法。

[0058] 进而，在本说明书中，公开应用上述的安全地更新模板的方法来防止重放攻击的方法。

[0059] 在本说明书中，基本上新公开在本申请申请人公开了的专利文献1的数据处理装置中，安全地更新模板的方法，能够应用于专利文献1的实施方式2以及4记载的“通过特征矢量的汉明距离或者欧几里得平方距离进行生物体认证”的认证方法。

[0060] 因此，在本说明书中，在实施方式1中，说明专利文献1的实施方式2记载的方式中的模板的更新方法，在实施方式2中，说明专利文献1的实施方式4记载的方式中的模板的更新方法。

[0061] 而且，关于在实施作为模板更新的应用的重放攻击对策的方法，在本说明书的实施方式3和4中进行说明。

[0062] 另外，作为实施方式1以及实施方式3的补充说明，将成为实施方式1以及实施方式3的方法的前提的专利文献1的实施方式2记载的认证方法的要旨作为实施方式5示出。

[0063] 另外，作为实施方式2以及实施方式4的补充说明，将成为实施方式2以及实施方式

4的方法的前提的专利文献1的实施方式4记载的认证方法的要旨作为实施方式6示出。

[0064] 此处，限定于本说明书的实施方式1以及3所需的范围，说明非 专利文献1的冈本-高岛密码的算法。

[0065] 冈本-高岛密码是使用了使用椭圆曲线来定义的双对配对矢量空间的双重准同态密码。

[0066] 虽然考虑了多个构成该双对配对矢量空间的方法，但此处根据通过椭圆曲线的直积构成的方法进行说明。

[0067] 另外，将椭圆曲线上的群的运算一般记述为加法群的运算的情况较多，但此处还包括有限体上的运算而全部记述为乘法群。

[0068] 另外，依照使用了非对称配对的更一般的方式记述。

[0069] 将G、$G\hat{}$、G_T分别设为素数位数q的群。

[0070] 设为$F_q=\{0,1,\cdots,q-1\}$。

[0071] 将$e:G\times G\hat{}\rightarrow G_T$设为满足双线型性(相对任意的$u\in G$，$v\hat{}\in G\hat{}$，$a,b\in F_q$成为$e(u^a,v\hat{}^b)=e(u,v\hat{})^{ab}$的性质)以及非退化性(存在是$e(g,g\hat{})\neq 1$那样的$g\in G$，$g\hat{}\in G\hat{}$的性质)的配对。

[0072] 将N个群G的直积集合设为$V=G\times G\times\cdots\times G$，同样地将$N$个群$G\hat{}$的直积集合设为$V\hat{}=G\hat{}\times G\hat{}\times\cdots\times G\hat{}$。

[0073] 此时，式1所示的关系成立。

[0074] 【式1】

[0075] 如果相对

[0076] $x=(g^{x1},g^{x2},\cdots,g^{xN})\in V$，$y=(g^{y1},g^{y2},\cdots,g^{yN})\in V$，$\alpha\in F_q$

[0077] 定义为

[0078] $x+y=(g^{x1+y1},g^{x2+y2},\cdots,g^{xN+yN})$

[0079] $\alpha x=(g^{\alpha x1},g^{\alpha x2},\cdots,g^{\alpha xN})$

[0080] 则V构成矢量空间。

[0081] 同样地，

[0082] 如果相对

[0083] $\hat{\mathbf{x}}=(\hat{g}^{x1},\hat{g}^{x2},\ldots,\hat{g}^{xN})\in\hat{V}$，$\hat{\mathbf{y}}=(\hat{g}^{y1},\hat{g}^{y2},\ldots,\hat{g}^{yN})\in\hat{V}$，$\alpha\in F_q$

[0084] 定义为

[0085] $\hat{\mathbf{x}}+\hat{\mathbf{y}}=(\hat{g}^{x1+y1},\hat{g}^{x2+y2},\ldots,\hat{g}^{xN+yN})$

[0086] $\alpha\hat{\mathbf{x}}=(\hat{g}^{\alpha x1},\hat{g}^{\alpha x2},\ldots,\hat{g}^{\alpha xN})$

[0087] 则$\hat{V}$构成矢量空间。

[0088] 另外，在本说明书中，设为$\hat{G},\hat{g},\hat{v}$等在文字上附加了“^”的记号与$G\hat{}$、$g\hat{}$、$v\hat{}$等在文字的旁边附加了“^”的记号相同。关于后述$A\hat{}$，$C\hat{}$，$a\hat{}$，$c\hat{}$，$d\hat{}$，$w\hat{}$等也是同样的。

[0089] 作为2个矢量空间V、$V\hat{}$的配对，

[0090] 如式2那样定义针对$u=(u_1,u_2,\cdots,u_N)\in V$，$v\hat{}=(v\hat{}_1,v\hat{}_2,\cdots,v\hat{}_N)\in V\hat{}$的配对。

[0091] 【式2】

[0092] $e(\mathbf{u},\hat{\mathbf{v}})=\prod_{i=1}^{N}e(u_i,\hat{v}_i)$

[0093] 在矢量空间V、V^中，式3所示的关系成立。

[0094] 【式3】

[0095] 如果设为

[0096] $a_1=(g,1,1,\cdots,1),a_2=(1,g,1,\cdots,1),\cdots,a_N=(1,1,1,\cdots,g)$

[0097] $\hat{\mathbf{a}}_1=(\hat{g},1,1,\ldots,1),\hat{\mathbf{a}}_2=(1,\hat{g},1,\ldots,1),\ldots,\hat{\mathbf{a}}_N=(1,1,1,\ldots,\hat{g})$

[0098] 则$A=(a_1,a_2,\cdots,a_N)$，$\hat{\mathbf{A}}=(\hat{\mathbf{a}}_1,\hat{\mathbf{a}}_2,\ldots,\hat{\mathbf{a}}_N)$分别成为矢量空间V，$\hat{V}$的基底。另外，A，$\hat{\mathbf{A}}$满足$e(\mathbf{a}_i,\hat{\mathbf{a}}_j)=e(g,\hat{g})^{\delta_{i,j}}$。

[0099] 此处$\delta_{i,j}$是克罗内克的德尔塔(Kronecker's delta)。将该基底A，$\hat{\mathbf{A}}$称为标准基底。

[0100] 设为$x=x_1a_1+x_2a_2+\cdots+x_Na_N\in V$。

[0101] 将矢量空间V中的失真映射$\varphi_{i,j}$：$\mathbf{V}\rightarrow\mathbf{V}$定义为$\varphi_{i,j}(\mathbf{x})=\mathbf{x}_j\mathbf{a}_i$。

[0102] 同样地，针对$x\hat{}=x_1a\hat{}_1+x_2a\hat{}_2+\cdots+x_Na\hat{}_N\in V\hat{}$，将$\hat{\varphi}_{i,j}$：$\hat{\mathbf{V}}\rightarrow\hat{\mathbf{V}}$定义为$\hat{\varphi}_{i,j}(\hat{\mathbf{x}})=\mathbf{x}_j\hat{\mathbf{a}}_i$。

[0103] 这样的失真映射能够容易地计算。

[0104] 这样，将有标准基底、定义了空间彼此的配对、定义了可计算的 失真映射的2个矢量空间称为双对配对矢量空间。

[0105] 将$X=(X_{i,j})$，$X\hat{}=(X\hat{}_{i,j})$设为各要素由从F_q均匀随机地选择了的值构成的N行N列的方阵。

[0106] 这样构成了的X，X^以极其高的概率成为正则矩阵。

[0107] 如果使用这样的正则矩阵如式4所示地定义，则$W=(w_1,w_2,\cdots,w_N)$，$W\hat{}=(w\hat{}_1,w\hat{}_2,\cdots,w\hat{}_N)$也成为基底。将该基底称为随机基底。

[0108] 【式4】

[0109] $\mathbf{w}_i=\sum_{j=1}^{N}\chi_{i,j}\mathbf{a}_j,\hat{\mathbf{w}}_i=\sum_{j=1}^{N}\hat{\chi}_{i,j}\hat{\mathbf{a}}_j$

[0110] 根据非专利文献2，关于矢量空间V，V^中的随机基底$W=(w_1,w_2,\cdots,w_N)$，$W\hat{}=(w\hat{}_1,w\hat{}_2,\cdots,w\hat{}_N)$，以下的性质成立。

[0111] 在提供了F^N_q的要素$(x_1,x_2,\cdots,x_N)$时，易于得到$x=x_1w_1+x_2w_2+\cdots+x_Nw_N$，$x\hat{}=x_1w\hat{}_1+x_2w\hat{}_2+\cdots+x_Nw\hat{}_N$。

[0112] 但是，已知在提供了$x=x_1w_1+x_2w_2+\cdots+x_Lw_L$，$x\hat{}=x_1w\hat{}_1+x_2w\hat{}_2+\cdots+x_Lw\hat{}_L$($1<L\leqslant N$)时，不使用$X=(X_{i,j})$，$X\hat{}=(X\hat{}_{i,j})$而得到矢量$y=x_1w_1+x_2w_2+\cdots+x_1w_1$，$y\hat{}=x_1w\hat{}_1+x_2w\hat{}_2+\cdots+x_1w\hat{}_1$($1\leqslant l<L$)有与一般化了的Diffie-Hellman计算问题相同的程度的难度。

[0113] 另一方面，如果使用$X=(X_{i,j})$，$X\hat{}=(X\hat{}_{i,j})$，则能够通过以下的算法Deco(式5)，容易地计算上述那样的矢量分解。另外，式5中的k是整数。

[0114] 【式5】

[0115] $Deco(x,\langle w_1,\cdots,w_1\rangle,X)$：

[0116] $(t_{i,j}) \leftarrow X^{-1}$

[0117] $\mathbf{y} \leftarrow \sum_{i=1}^{L}\sum_{j=1}^{l}\sum_{k=1}^{L} t_{i,j} x_{j,k} \phi_{k,i}(\mathbf{x})$

[0118] $\mathbf{Deco}\left(\hat{\mathbf{x}}, <\hat{\mathbf{w}}_1,\ldots,\hat{\mathbf{w}}_l>, \hat{X}\right)$：

[0119] $(\hat{t}_{i,j}) \leftarrow \hat{X}^{-1}$

[0120] $\hat{\mathbf{y}} \leftarrow \sum_{j=1}^{L}\sum_{j=1}^{l}\sum_{k=1}^{L} \hat{t}_{i,j} \hat{x}_{j,k} \hat{\phi}_{k,i}(\hat{\mathbf{x}})$

[0121] 根据该性质，能够通过将正则矩阵作为秘密密钥而实现陷门函数。

[0122] 以下，说明在使用了双对配对矢量空间的数据处理装置中，安全地更新模板的方法。

[0123] 实施方式1.

[0124] 在本实施方式中，说明在使用上述冈本-高岛准同态密码对特征矢量进行加密，根据特征矢量的汉明距离或者欧几里得平方距离进行生物体认证的数据处理装置中，安全地更新模板的方法。

[0125] 图1是示出实施方式1-4的生物体认证系统的结构例的图。

[0126] 在图1中，证明装置101是从用户测定生物体信息，并使用所测定了的生物体信息来进行隐匿核对处理的装置。

[0127] 认证装置102是预先对用户的生物体信息进行加密而储存，并且使用所储存了的加密了的生物体信息来进行认证的装置。

[0128] 解密装置103是对加密类似度信息进行解密的装置。

[0129] 另外，证明装置101是密码装置的例子，认证装置是数据处理装置的例子。

[0130] 图2是示出证明装置101的内部结构的结构例的图。

[0131] 在图2中，生物体信息抽出部201使用光学照相机、红外线照相机等各种传感器，从生物体抽出为了进行个人识别而所需的信息。

[0132] 特征矢量形成部202从由生物体信息抽出部201抽出了的生物体信息，形成表示个人的特征的特征矢量。

[0133] 随机数生成部203生成随机数。

[0134] 加密部204对特征矢量进行加密。

[0135] 存储部205储存公开密钥等各种数据。

[0136] 通信部206在与数据库等其他装置之间进行数据的发送接收。

[0137] 图3是示出认证装置102的内部结构的结构例的图。

[0138] 在图3中，存储部301储存加密了的特征矢量(以下还称为加密特征矢量)、公开密钥等各种数据。

[0139] 存储部301存储的加密特征矢量是由证明装置101加密了的登记用的特征矢量，在认证时被用作模板。

[0140] 在本说明书中，加密特征矢量还记载为模板、加密生物体信息。

[0141] 另外，加密前的登记用的特征矢量(加密前的登记用的生物体信息)相当于第1数据的例子，存储部301存储的加密特征矢量(模板、加密生物体信息)相当于加密第1数据的例子。

[0142] 另外，如后所述，在由模板更新部307更新了加密特征矢量的情况下，存储部301盖写现有的加密特征矢量(从证明装置101取得了的加密特征矢量或者通过上次的更新得到的加密特征矢量)，存储更新了的加密特征矢量。

[0143] 另外，存储部301存储的公开密钥是由解密装置103生成并从解密装置103分发了的公开密钥。

[0144] 另外，如后所述，在由公开密钥更新部306更新了公开密钥的情况下，盖写现有的公开密钥(从解密装置103取得了的公开密钥或者通过上次的更新得到的公开密钥)，存储更新了的公开密钥。

[0145] 另外，存储部301相当于加密数据存储部以及公开密钥存储部的例子。

[0146] 加密类似度生成部302根据登记了的加密特征矢量、和认证用的加密特征矢量，生成加密类似度信息。

[0147] 认证用的加密特征矢量是由证明装置101加密了的认证用的特征矢量。

[0148] 加密前的认证用的特征矢量相当于第2数据的例子，认证用的加密特征矢量相当于加密第2数据的例子。

[0149] 另外，加密类似度信息是通过使用了与公开密钥对应起来的秘密密钥的解密处理能够在解密装置103中导出登记用的特征矢量(第1数据)与认证用的特征矢量(第2数据)之间的类似度的加密了的信 息。

[0150] 另外，在后述实施方式5以及6中，详细说明加密类似度生成部302。

[0151] 判定部303根据类似度进行个人识别，判定是否为本人。

[0152] 通信部304在与证明装置101、解密装置103之间进行数据的发送接收。

[0153] 例如，通信部304在认证时，从证明装置101接收认证用的加密特征矢量。

[0154] 如上所述，加密特征矢量相当于加密第2数据的例子，所以通信部304相当于加密数据输入部的例子。

[0155] 另外，通信部304有时如后述实施方式3以及4所示，从证明装置101接收认证要求。

[0156] 例如，在需要用户的认证时，从证明装置101向认证装置102发送认证要求。

[0157] 例如，在证明装置101设置于银行的ATM的情况下，在银行的顾客开始ATM的利用时，从证明装置101发送到认证装置102。

[0158] 如后所述，在从证明装置101有认证要求的情况下，在认证装置102中通过公开密钥更新部306更新公开密钥，将更新了的公开密钥发送到证明装置101。

[0159] 按照该意思，认证要求是要求公开密钥的供给的要求，认证要求相当于公开密钥供给要求的例子。

[0160] 因此，通信部304还是公开密钥供给要求输入部的例子。

[0161] 随机数生成部305生成随机数。

[0162] 更具体而言，随机数生成部305每当发生规定的触发事件时，使用在触发事件发生时在存储部301中存储的公开密钥的至少一部分，生成随机数。

[0163] 例如，可以考虑将从证明装置101的认证要求的接收、公开密钥以及加密特征矢量的周期性的更新定时的到来等作为触发事件。

[0164] 另外，也可以将系统管理者对认证装置102指示了公开密钥、加 密特征矢量的更新作为触发事件的发生。

[0165] 公开密钥更新部306每当由随机数生成部305生成了随机数时，进行使用了由随机数生成部305生成了的随机数的运算，更新在触发事件发生时在存储部301中存储的公开密钥。

[0166] 模板更新部307每当由随机数生成部305生成了随机数时，进行使用了由随机数生成部305生成了的随机数的运算，更新在触发事件发生时在存储部301中存储的模板(加密第1数据)。

[0167] 模板更新部307相当于加密数据更新部的例子。

[0168] 图4是示出解密装置103的内部结构的结构例的图。

[0169] 在图4中，参数生成部401生成公开密钥、秘密密钥等加密和解密所需的参数。

[0170] 解密部402对加密类似度信息进行解密，取出明文的类似度。

[0171] 存储部403储存公开密钥、秘密密钥等各种数据。

[0172] 通信部404在与数据库等其他装置之间进行数据的发送接收。

[0173] 接下来，说明本实施方式的数据处理方法。

[0174] 首先，说明动作的概要。

[0175] 动作被分成设置处理、登记处理、认证处理、模板更新处理这4个。

[0176] 在设置处理中，解密装置103生成加密和解密所需的参数。

[0177] 在登记处理中，证明装置101对用户的生物体信息进行加密而送到认证装置102，认证装置102储存到存储部301中。

[0178] 在认证处理中，首先证明装置101对用户的生物体信息进行加密而将认证用的加密生物体信息送到认证装置102。接下来，认证装置102使用存储部301的加密生物体信息(模板)和接受了的加密生物体信息来生成加密类似度信息，将加密类似度信息送到解密装置103。接下来，解密装置103对类似度进行解密，向认证装置102送出解密了的类似度。最后，认证装置102比较类似度和阈值，进行认证。

[0179] 在模板更新处理中，认证装置102更新公开密钥和模板，公开新的公开密钥。

[0180] 另外，在本说明书中，关于设置处理、登记处理、认证处理，包括记号而如专利文献1记载。

[0181] 在实施方式5中，详细说明设置处理、登记处理、认证处理，在实施方式1中，仅说明模板的更新处理。

[0182] 使用图5，详细说明模板的更新处理。

[0183] 图5是示出模板的更新步骤的流程图。

[0184] 在发生了触发事件的情况下，首先，在步骤S501中，随机数生成部305从0至q-1的整数中均匀随机地取出值δ。

[0185] 值δ是随机数值。

[0186] 另外，上述“均匀”是指，0至q-1的各值的出现概率相同。

[0187] 此处，上述“q”是群位数。

[0188] 如在实施方式5中说明的图9的S906所示，是公开密钥pk＝(q、V、V^、e、G_T、A、A^、W、W^、e(g,g^))，群位数q是公开密钥pk的一部分(构成要素)。

[0189] 即，随机数生成部305使用公开密钥pk的一部分来生成随机数。

[0190] 接下来，在步骤S502中，公开密钥更新部306使用现有的公开密钥参数e(g,g^)和

随机基底$W=(w_1、w_2、w_3)$、$\hat{W}=(\hat{w}_1、\hat{w}_2、\hat{w}_3)$和随机数值δ，决定新的公开密钥参数$e(g,\hat{g})^+=e(\delta g,\delta\hat{g})$、随机基底$W^+=(\delta w_1、\delta w_2、\delta w_3)$、$\hat{W}^+=(\delta\hat{w}_1、\delta\hat{w}_2、\delta\hat{w}_3)$。

[0191] 如上所述，公开密钥$pk=(q、V、\hat{V}、e、G_T、A、\hat{A}、W、\hat{W}、e(g,\hat{g}))$，公开密钥参数$e(g,\hat{g})$和随机基底W以及$\hat{W}$是公开密钥pk的一部分。

[0192] 这样，从现有的公开密钥参数$e(g,\hat{g})$和随机基底W以及$\hat{W}$更新为新的公开密钥参数$e(g,\hat{g})^+$和随机基底W^+以及$\hat{W}^+$是与从现有的公开密钥pk更新为新的公开密钥pk^+相同的含义。

[0193] 接下来，在步骤S503中，模板更新部307使用现有的模板$C=(c_1,c_2,\cdots,c_T)$和随机数值δ，计算新的模板$C^+=(\delta c_1,\delta c_2,\cdots,\delta c_T)$。

[0194] 然后，存储部301盖写现有的模板C，存储新的模板C^+。

[0195] 另外，此时，存储部301盖写公开密钥参数$e(g,\hat{g})$和随机基底W以及$\hat{W}$，存储由公开密钥更新部306生成了的新的公开密钥参数$e(g,\hat{g})^+$和随机基底W^+以及$\hat{W}^+$。

[0196] 存储新的公开密钥参数$e(g,\hat{g})^+$和随机基底W^+以及$\hat{W}^+$相当于盖写现有的公开密钥pk而存储新的公开密钥pk^+。

[0197] 接下来，在步骤S504中，模板更新部307删除随机数值δ。

[0198] 最后，在步骤S505中，公开新的公开密钥参数$e(g,\hat{g})^+$和随机基底$W^+=(\delta w_1、\delta w_2、\delta w_3)$、$\hat{W}^+=(\delta\hat{w}_1、\delta\hat{w}_2、\delta\hat{w}_3)$。

[0199] 步骤S505通过例如通信部304将新的公开密钥参数$e(g,\hat{g})^+$和随机基底W^+以及$\hat{W}^+$发送到证明装置101以及解密装置103而实现。

[0200] 在证明装置101以及解密装置103中，能够使用新的公开密钥参数$e(g,\hat{g})^+$和随机基底W^+以及$\hat{W}^+$来生成新的公开密钥pk^+，发送新的公开密钥参数$e(g,\hat{g})^+$和随机基底W^+以及$\hat{W}^+$是与发送新的公开密钥pk^+相同的含义。

[0201] 另外，通信部304也可以代替发送新的公开密钥参数$e(g,\hat{g})+$和随机基底W^+以及$\hat{W}^+$，而对证明装置101以及解密装置103发送新的公开密钥pk^+。

[0202] 另外，也可以代替利用通信部304的发送，而在可移动存储介质中储存新的公开密钥参数$e(g,\hat{g})^+$和随机基底W^+以及$\hat{W}^+$(或者新的公开密钥pk^+)，使证明装置101以及解密装置103从该可移动存储介质读入新的公开密钥参数$e(g,\hat{g})^+$和随机基底W^+以及$\hat{W}^+$(或者新的公开密钥pk^+)。

[0203] 以后，使用新的公开密钥pk^+和新的模板C^+，进行依照专利文献1的实施方式2(即本说明书的实施方式5)所示的步骤的认证处理。

[0204] 即，首先证明装置101使用新的公开密钥pk^+对用户的生物体信息进行加密而将认证用的加密生物体信息送到认证装置102。

[0205] 接下来，认证装置102使用存储部301的加密生物体信息(新的模板C^+)、接受了的加密生物体信息、以及存储部301的新的公开密 钥pk^+来生成加密类似度信息，将加密类似度信息送到解密装置103。

[0206] 接下来，解密装置103使用秘密密钥sk和新的公开密钥pk^+对类似度进行解密，对认证装置102送出解密了的类似度。

[0207] 最后，认证装置102比较类似度和阈值，进行认证。

[0208] 另外，即使在图5所示的步骤中公开密钥和模板被更新，秘密密钥sk也不被更新。

[0209] 在算法的性质上，即使秘密密钥sk未被更新，解密装置103也能够进行类似度的解密。

[0210] 如果通过以上的步骤更新模板和公开密钥，则即使假设旧模板被泄漏，也无法使用旧模板来对认证装置102冒充。

[0211] 其原因为，作为公开密钥的一部分的公开密钥参数和随机基底已经被置换为新的公开密钥参数$e(g,g\hat{})^{+}$和随机基底$W^{+}=(\delta w_1、\delta w_2、\delta w_3)$、$W\hat{}^{+}=(\delta w\hat{}_1、\delta w\hat{}_2、\delta w\hat{}_3)$，在解密装置103中的解密处理中也使用该新的公开密钥参数和随机基底，所以在新的公开密钥参数、随机基底、以及旧模板之间，产生不一致，该不一致反映到汉明距离、欧几里得平方距离的解密结果，成为与随机数值δ对应的随机的值。

[0212] 另外，如果通过以上的步骤更新模板和公开密钥，则即使获得了旧模板、新公开密钥参数、以及随机基底，也无法计算新模板。

[0213] 其原因为，该计算问题回到了在计算量逻辑的领域中成为难以计算的问题之一的“计算Diffie-Hellman问题”。

[0214] 以上，说明了实施方式1。

[0215] 根据该实施方式1，具有在使用了冈本-高岛准同态密码的数据处理装置中，能够安全地更新模板这样的效果。

[0216] 因此，即使在模板泄漏了的情况下，也能够有效地对抗使用了泄漏了的模板的“冒充”，能够提高保密强度。

[0217] 另外，根据该实施方式1，由于使用了冈本-高岛准同态密码，所以相比于使用BGN密码的情况，具有能够减小群的规模，能够加快运算这样的效果。

[0218] 实施方式2.

[0219] 在本实施方式中，说明在使用了非专利文献3所示的BGN(Boneh-Goh-Nissim)密码的数据处理装置中，安全地更新模板的方法。

[0220] 另外，本实施方式的生物体认证系统的结构例也如图1所示。

[0221] 另外，本实施方式的证明装置101、认证装置102、解密装置103的内部结构例也如图2-图4所示。

[0222] 首先，说明BGN密码的算法。

[0223] BGN密码也是双重准同态密码中的一个。

[0224] BGN密码由密钥生成、加密、解密这3个算法构成。

[0225] 密钥生成算法如以下所述。

[0226] 将p、q分别设为素数。

[0227] 作为$N=pq$，生成以N为位数(order)的群G、G_T。

[0228] 将$e:G\times G\rightarrow G_T$设为满足双线型性以及非退化性的配对。

[0229] 将g、u设为从G均匀随机地选择了的要素。

[0230] 通过$h=u^{q}$，决定h。

[0231] 另外，将公开密钥设为$((G,G_T,N,e)、g、h、e(g,g))$，将秘密密钥设为p。

[0232] 加密算法如以下所述。

[0233] 另外，将明文空间设为{0、1、…、L}。

[0234] 从{0、1、…、N-1}均匀随机地选择r。

[0235] 将针对x的密文E(x)设为$E(x)=g^{x}h^{r}$。

[0236] 解密算法如以下所述。

[0237] 如果将密文设为E(x),则首先使用秘密密钥p来计算$E(x)^{p}$。

[0238] 根据定义,成为$E(x)^{p}=(g^{x}h^{r})^{p}=(g^{p})^{x}$。

[0239] 然后,针对该值,求出以g^{p}为底的离散对数,得到原来的明文x。另外,g是作为公开密钥的一部分从解密装置103分发的。

[0240] 另外,求出离散对数的计算在当前的计算机能力下是困难的,但 在已知明文空间的大小L小的情况下,通过使用Pollard的LAMBDA法能够以$\sqrt{L}$程度的计算量计算。

[0241] 说明在使用了这样的BGN密码的数据处理装置中,安全地更新模板的方法。

[0242] 另外,在本说明书中,关于设置处理、登记处理、认证处理,还包括记号而如专利文献1所述。

[0243] 在实施方式6中,详细说明设置处理、登记处理、认证处理,在实施方式2中,仅说明模板的更新处理。

[0244] 使用图6,详细说明模板的更新。

[0245] 图6是示出模板的更新步骤的流程图。

[0246] 在发生了触发事件的情况下,首先,在步骤S601中,随机数生成部305从0至q-1的整数中均匀随机地取出值δ。

[0247] 值δ是随机数值。

[0248] 另外,上述“均匀”是指,0至q-1的各值的出现概率相同。

[0249] 如上所述,“q”是素数。

[0250] 如在实施方式6中说明的图14的S1301所示,N=pq,并且,如图14的S1303所示,公开密钥$pk=((G,G_{T},N,e),g,h,e(g,g))$,素数q是公开密钥pk的一部分(构成要素)。

[0251] 即,随机数生成部305使用公开密钥pk的一部分来生成随机数。

[0252] 接下来,在步骤S602中,公开密钥更新部306使用现有的公开密钥$((G,G_{T},N,e),g,h,e(g,g))$和随机数值δ,决定新的公开密钥$((G,G_{T},N,e),g^{\delta},h^{\delta},e(g,g)^{\delta\hat{}2})$。

[0253] 接下来,在步骤S603中,模板更新部307使用现有的模板$C=(c_{1},c_{2},\cdots,c_{T})$和随机数值δ,计算新的模板$C^{+}=(c^{\delta}_{1},c^{\delta}_{2},\cdots,c^{\delta}_{T})$。

[0254] 然后,存储部301盖写现有的模板C,存储新的模板C^{+}。

[0255] 另外,此时,存储部301盖写现有的公开密钥$((G,G_{T},N,e),g,h,e(g,g))$,存储由公开密钥更新部306生成了的新的公开密钥$((G,G_{T},N,e),g^{\delta},h^{\delta},e(g,g)^{\delta\hat{}2})$。

[0256] 接下来,在步骤S604中,模板更新部307删除随机数值δ。

[0257] 最后,在步骤S605中,公开新的公开密钥$((G,G_{T},N,e),g^{\delta},h^{\delta},e(g,g)^{\delta\hat{}2})$。

[0258] 步骤S605通过例如通信部304将新的公开密钥$((G,G_{T},N,e),g^{\delta},h^{\delta},e(g,g)^{\delta\hat{}2})$发送到证明装置101以及解密装置103而实现。

[0259] 另外,也可以代替利用通信部304的发送,在可移动存储介质中储存新的公开密钥$((G,G_{T},N,e),g^{\delta},h^{\delta},e(g,g)^{\delta\hat{}2})$,使证明装置101以及解密装置103从该可移动存储介质读入新的公开密钥$((G,G_{T},N,e),g^{\delta},h^{\delta},e(g,g)^{\delta\hat{}2})$。

[0260] 以后,使用新的公开密钥$((G,G_{T},N,e),g^{\delta},h^{\delta},e(g,g)^{\delta\hat{}2})$和新的模板$C^{+}$,进行依照专利文献1的实施方式4(即本说明书的实施方式6)所示的步骤的认证处理。

[0261] 即，首先证明装置101使用新的公开密钥$((G,G_T,N,e),g^{\delta},h^{\delta},e(g,g)^{\delta\hat{}2})$对用户的生物体信息进行加密而将认证用的加密生物体信息送到认证装置102。

[0262] 接下来，认证装置102使用存储部301的加密生物体信息(新的模板C^{+})、接受了的加密生物体信息、以及存储部301的新的公开密钥$((G,G_T,N,e),g^{\delta},h^{\delta},e(g,g)^{\delta\hat{}2})$来生成加密类似度信息，将加密类似度信息送到解密装置103。

[0263] 接下来，解密装置103使用秘密密钥sk和新的公开密钥$((G,G_T,N,e),g^{\delta},h^{\delta},e(g,g)^{\delta\hat{}2})$对类似度进行解密，向认证装置102送出解密了的类似度。

[0264] 最后，认证装置102比较类似度和阈值，进行认证。

[0265] 另外，即使在图6所示的步骤中公开密钥和模板被更新，秘密密钥sk也不会被更新。

[0266] 在算法的性质上，即使秘密密钥sk未被更新，解密装置103也能够进行类似度的解密。

[0267] 如果通过以上的步骤更新模板和公开密钥，则即使假设旧模板被 泄漏，也无法使用旧模板来对认证装置102冒充。

[0268] 其原因为，公开密钥已经被置换为新的公开密钥$((G,G_T,N,e),g^{\delta},h^{\delta},e(g,g)^{\delta\hat{}2})$，在解密装置103中的解密处理中也使用了该新的公开密钥，所以在新的公开密钥与旧模板之间产生不一致，该不一致反映到汉明距离、欧几里得平方距离的解密结果，成为与随机数值δ对应的随机的值。

[0269] 另外，如果通过以上的步骤更新模板和公开密钥，则即使获得了旧模板和新随机基底，也无法计算新模板。

[0270] 其原因为，该计算问题回到了在计算量逻辑的领域中成为难以计算的问题之一的“计算Diffie-Hellman问题”。

[0271] 以上，说明了实施方式2。

[0272] 根据该实施方式2，具有在使用了BGN密码的数据处理装置中，能够安全地更新模板这样的效果。

[0273] 因此，即使在模板泄漏了的情况下，也能够有效地对抗使用了泄漏了的模板的“冒充”，能够提高保密强度。

[0274] 另外，根据该实施方式2，由于使用了BGN密码，所以具有相比于实施方式1能够减小模板的规模这样的效果。

[0275] 实施方式3.

[0276] 在本实施方式中，说明使用实施方式1的模板的更新方法来实施重放攻击对策的方法。

[0277] 系统结构以及各装置的结构如图1至图4所示，所以此处省略记述。

[0278] 使用图7，详细说明使用实施方式1的模板的更新方法来实施重放攻击对策的方法。

[0279] 图7是示出使用实施方式1的模板的更新方法来实施重放攻击对策的情况的步骤的流程图。

[0280] 在图7中，证明装置101在步骤S701中发送认证要求。

[0281] 接受到认证要求的认证装置102在步骤S702中，随机数生成部305从0至q-1的整数

中均匀随机地取出值δ。

[0282] 接下来，在步骤S703中，公开密钥更新部306使用现有的公开密钥参数$e(g,g\hat{})$和随机基底$W=(w_1、w_2、w_3)$、$W\hat{}=(w\hat{}_1、w\hat{}_2、w\hat{}_3)$和随机数值δ，决定新的公开密钥参数$e(g,g\hat{})^{+}=e(\delta g,\delta g\hat{})$和随机基底$W^{+}=(\delta w_1、\delta w_2、\delta w_3)$、$W\hat{}^{+}=(\delta w\hat{}_1、\delta w\hat{}_2、\delta w\hat{}_3)$。

[0283] 接下来，在步骤S704中，模板更新部307使用现有的模板$C=(c_1,c_2,\cdots,c_T)$和随机数值δ，计算新的模板$C^{+}=(\delta c_1,\delta c_2,\cdots,\delta c_T)$，存储部301盖写现有的模板，存储新的模板$C^{+}$。

[0284] 另外，存储部301盖写现有的公开密钥参数$e(g,g\hat{})$和随机基底W以及$W\hat{}$，存储新的公开密钥参数$e(g,g\hat{})^{+}$和随机基底W^{+}以及$W\hat{}^{+}$。

[0285] 接下来，在步骤S705中，模板更新部307删除随机数值δ。

[0286] 接下来，在步骤S706中，公开新的公开密钥参数$e(g,g\hat{})^{+}$和随机基底$W^{+}=(\delta w_1、\delta w_2、\delta w_3)$、$W\hat{}^{+}=(\delta w\hat{}_1、\delta w\hat{}_2、\delta w\hat{}_3)$。

[0287] 如果接受了该新的公开密钥参数和随机基底，则证明装置101在步骤S707以后，将包括新的公开密钥参数和随机基底的公开密钥作为新公开密钥，通过专利文献1的实施方式2(即本说明书的实施方式5)记载的认证方法进行认证。

[0288] 如果通过以上的步骤进行认证处理，则每当认证时(每当发送认证要求时)生成新的公开密钥，所以能够防止重放攻击。

[0289] 以上，说明了实施方式3。

[0290] 根据该实施方式3，能够使用实施方式1记载的模板的更新方法来实施重放攻击对策，无需追加新的装置，所以具有相比于另外实施重放攻击对策能够降低成本这样的效果。

[0291] 实施方式4.

[0292] 在本实施方式中，说明使用实施方式2的模板的更新方法来实施重放攻击对策的方法。

[0293] 系统结构以及各装置的结构如图1至图4所示，所以此处省略记述。

[0294] 使用图8，详细说明使用实施方式2的模板的更新方法来实施重 放攻击对策的方法。

[0295] 图8是示出使用实施方式2的模板的更新方法来实施重放攻击对策的情况的步骤的流程图。

[0296] 在图8中，证明装置101在步骤S801中发送认证要求。

[0297] 在接受了认证要求的认证装置102中，在步骤S802中，随机数生成部305从0至q-1的整数中均匀随机地取出值δ。

[0298] 接下来，在步骤S803中，公开密钥更新部306使用公开密钥$((G,G_T,N,e),g,h,e(g,g))$和随机数值δ，决定新的公开密钥$((G,G_T,N,e),g^{\delta},h^{\delta},e(g,g)^{\delta\hat{}2})$。

[0299] 接下来，在步骤S804中，模板更新部307使用现有的模板$C=(c_1,c_2,\cdots,c_T)$和随机数值δ，计算新的模板$C^{+}=(c^{\delta}_1,c^{\delta}_2,\cdots,c^{\delta}_T)$，存储部301盖写现有的模板，存储新的模板$C^{+}$。

[0300] 另外，存储部301盖写现有的公开密钥，存储新的公开密钥。

[0301] 接下来，在步骤S805中，模板更新部307删除随机数值δ。

[0302] 接下来，在步骤S806中，公开新的公开密钥$((G,G_T,N,e),g^{\delta},h^{\delta},e(g,g)^{\delta\hat{}2})$。

[0303] 如果接受了该新的公开密钥，则证明装置101在步骤S807以后，使用新公开密钥，通过专利文献1的实施方式4(即本说明书的实施方式6)记载的认证方法进行认证。

[0304] 如果通过以上的步骤进行认证处理，则每当认证时(每当发送认证要求时)生成新的公开密钥，所以能够防止重放攻击。

[0305] 以上，说明了实施方式4。

[0306] 根据该实施方式4，能够使用实施方式2记载的模板的更新方法来实施重放攻击对策，无需追加新的装置，所以具有相比于另外实施重放攻击对策能够降低成本这样的效果。

[0307] 以上，在实施方式1以及实施方式2中说明了模板的更新方法，在实施方式3以及实施方式4中说明了使用实施方式1以及实施方式2中说明了模板的更新方法的重放攻击对策方法。

[0308] 另外，当然能够组合它们来利用。

[0309] 即，能够每当认证时实施重放攻击对策，进而在有模板的泄漏的危险时实施模板更新。

[0310] 实施方式5.

[0311] 在实施方式5中，为了补充实施方式1以及实施方式3的说明，说明专利文献1的实施方式2记载的方式中的设置处理、登记处理、认证处理。

[0312] 在专利文献1的实施方式2记载的方式中，准备T个数组，由此构成特征矢量，但此时，作为类似度的指标，使用2个特征矢量的汉明距离或者欧几里得平方距离。

[0313] 将2个特征矢量设为$b=(b_1,b_2,\cdots,b_T)$、$b'=(b'_1,b'_2,\cdots,b'_T)$。

[0314] 此时，通过式6提供2个特征矢量的汉明距离(其中$b_i,b'_i\in\{0,1\}$)，并且，通过式7提供2个特征矢量的欧几里得平方距离。

[0315] 【式6】

[0316] $$d_H(b,b')=\sum_{i=1}^{T}(b_i\oplus b'_i)=\sum_{i=1}^{T}(b_i-b'_i)^2$$

[0317] 【式7】

[0318] $$d_{E2}(b,b')=\sum_{i=1}^{T}(b_i-b'_i)^2$$

[0319] 接下来，使用图19-图22，说明专利文献1的实施方式2记载的方式中的设置处理、登记处理、认证处理各自的概要。

[0320] 图19示出设置处理的概要，图20示出登记处理的概要，图21以及图22示出认证处理的概要。

[0321] 首先，参照图19，说明设置处理的概要。

[0322] 最初，解密装置103的参数生成部401根据冈本-高岛密码算法，生成秘密密钥sk和公开密钥pk(S2101)。

[0323] 接下来，解密装置103的存储部403存储秘密密钥sk，通信部 404将公开密钥pk发送到证明装置101以及认证装置102(S2102)。

[0324] 接下来，在证明装置101中，通信部206接收公开密钥pk，存储部205存储公开密钥pk，在认证装置102中，通信部304接收公开密钥pk，存储部301存储公开密钥pk(S2102)。

[0325] 另外，此处，说明了对公开密钥pk进行发送接收的例子，但向证明装置101以及认证装置102分发公开密钥pk的方法也可以是其他方法。

[0326] 例如，也可以解密装置103将公开密钥pk储存到记录介质中，在证明装置101以及

认证装置102中从该记录介质读出并储存公开密钥pk。

[0327] 接下来，参照图20，说明登记处理的概要。

[0328] 最初，在证明装置101中，生物体信息抽出部201抽出用户的生物体信息(S2201)。

[0329] 接下来，证明装置101的特征矢量形成部202生成在S2201中抽出了的生物体信息的特征矢量b(S2202)。

[0330] 接下来，证明装置101的随机数生成部203使用公开密钥pk的一部分来生成随机数，并且加密部204从存储部205读出公开密钥pk，加密部204使用公开密钥pk和随机数而对特征矢量b进行加密(S2203)。

[0331] 接下来，证明装置101的通信部206将加密了的特征矢量C发送到认证装置102(S2204)。

[0332] 接下来，认证装置102的通信部304接收加密了的特征矢量C，存储部205存储加密了的特征矢量C(S2205)。

[0333] 接下来，参照图21以及图22，说明认证处理的概要。

[0334] 最初，在证明装置101中，生物体信息抽出部201抽出用户的生物体信息(S2301)。

[0335] 接下来，证明装置101的特征矢量形成部202生成在S2301中抽出了的生物体信息的特征矢量b'(S2302)。

[0336] 接下来，证明装置101的随机数生成部203使用公开密钥pk的 一部分来生成随机数，并且加密部204从存储部205读出公开密钥pk，加密部204使用公开密钥pk和随机数对特征矢量b'进行加密(S2303)。

[0337] 接下来，证明装置101的通信部206将加密了的特征矢量C^发送到认证装置102(S2304)。

[0338] 接下来，认证装置102的通信部304接收加密了的特征矢量C^(S2305)。

[0339] 接下来，认证装置102的加密类似度生成部302读出存储部301的加密特征矢量C(S2401)。

[0340] 接下来，认证装置102的随机数生成部305使用公开密钥pk的一部分来生成随机数，并且加密类似度生成部302从存储部301读出公开密钥pk，加密类似度生成部302针对从存储部301读出了的加密特征矢量C和从证明装置101接收了的加密特征矢量C^，使用公开密钥pk和随机数来生成加密类似度信息(S2402)。

[0341] 认证装置102不知道与公开密钥pk对应起来的秘密密钥sk，所以无法对加密特征矢量C以及加密特征矢量C^进行解密。因此，在加密特征矢量C以及加密特征矢量C^被加密了的状态下，生成加密类似度信息。

[0342] 接下来，认证装置102的通信部304将加密类似度信息发送到解密装置103(S2403)。

[0343] 接下来，解密装置103的通信部404接收加密类似度信息(S2404)。

[0344] 接下来，解密装置103的解密部402从参数生成部401读出秘密密钥sk，对加密类似度信息中使用秘密密钥sk来进行解密处理，导出明文的类似度(S2405)。

[0345] 接下来，解密装置103的通信部404将明文的类似度发送到认证装置102(S2406)。另外，类似度是表示登记用的特征矢量b和认证用的特征矢量b'类似到何种程度的信息，无法根据类似度计算特征矢量、生物体信息。

[0346] 接下来，认证装置102的通信部304接收明文的类似度(S2407)。

[0347] 接下来，认证装置102的判定部303判定明文的类似度是否为规定的阈值以上，如果是阈值以上则判定为是本人，在低于阈值的情况下，判定为并非本人(S2408)。

[0348] 以下，参照图9-图13，更详细地说明各处理的动作。

[0349] 图9示出设置处理的详细，图10示出登记处理的详细，图11-图13示出认证处理的详细。

[0350] 首先，使用图9来说明设置。

[0351] 在设置中，解密装置103生成公开密钥pk以及秘密密钥sk。

[0352] 该公开密钥pk以及秘密密钥sk既可以是针对每个用户不同的公开密钥以及秘密密钥，也可以是在系统中1个公开密钥以及秘密密钥。

[0353] 此处，为了简化说明，说明在系统中使用1个公开密钥以及秘密密钥的情况，但易于将其扩展到每个用户的公开密钥以及秘密密钥的情况。

[0354] 图9是示出参数生成部401中的公开密钥pk以及秘密密钥sk的生成步骤的流程图。

[0355] 首先，在步骤S901中，参数生成部401决定群位数q、群G、$G\hat{}$、G_T、生成元$g\in G$、$g\hat{}\in G\hat{}$。

[0356] 其具体的方法在例如非专利文献5中公开，所以此处省略。

[0357] 另外，群位数根据保密等级确定，通常成为200比特、1024比特等大的规模的素数。

[0358] 接下来，在步骤S902中，参数生成部401将矢量空间设为$V=G\times G\times G$、$V\hat{}=G\hat{}\times G\hat{}\times G\hat{}$，决定标准基底$A=(a_1,a_2,a_3)$，$A\hat{}=(a\hat{}_1,a\hat{}_2,a\hat{}_3)$。

[0359] 该决定方法如已经叙述的方法。

[0360] 接下来，在步骤S903中，参数生成部401从0至q-1的整数中均匀随机地取出9次值，使用它们来决定3行3列的矩阵$X=(X_{i,j})$。

[0361] 该矩阵必须是正则矩阵，但由于通过该方法决定矩阵，而以极其高的概率成为正则矩阵。另外，如果进一步期望正确性，则通过在这 样决定了矩阵之后计算矩阵式等方法判定正则性，如果并非正则，则再次随机地选择矩阵的要素即可。

[0362] 接下来，在步骤S904中，参数生成部401从0至q-1的整数中均匀随机地取出9次值，使用它们来决定3行3列的矩阵$X\hat{}=(X\hat{}_{i,j})$。

[0363] 该矩阵以极其高的概率成为正则矩阵，但在未成为正则矩阵的情况下，再次随机地选择即可。

[0364] 接下来，在步骤S905中，参数生成部401通过以下的式8以及式9，决定随机基底$W=(w_1,w_2,w_3)$，$W\hat{}=(w\hat{}_1,w\hat{}_2,w\hat{}_3)$。

[0365] 【式8】

[0366] $$\mathbf{w}_i=\sum_{j=1}^{3}\chi_{i,j}\mathbf{a}_j$$

[0367] 【式9】

[0368] $$\hat{\mathbf{w}}_i=\sum_{j=1}^{3}\hat{\chi}_{i,j}\hat{\mathbf{a}}_j$$

[0369] 最后，在步骤S906中，参数生成部401公开公开密钥$pk=(q、V、V\hat{}、e、G_T、A、A\hat{}、W、W\hat{}、e(g,g\hat{}))$，将秘密密钥$sk=(X、X\hat{})$储存到存储部403中。

[0370] 图10是示出在证明装置101中登记生物体信息的步骤的流程图。

[0371] 首先，在步骤S1001中，生物体信息抽出部201抽出用户的生物体信息。

[0372] 其中有各种方法，例如通过对指纹照射光并用传感器读取指纹型来抽出。

[0373] 接下来，在步骤S1002中，特征矢量形成部202根据生物体信息，形成特征矢量$b=(b_1,b_2,\cdots,b_T)$。

[0374] 此处，T是储存特征矢量的数组的大小，是通过特征矢量的形成方法决定的值。

[0375] 本实施方式的形成方法是指如下的方法：对所读取了的指纹型进 行区域分割，在各区域中检测有无特征点，在有特征点的部位的数组中储存1、并在无特征点的部位的数组中储存0，从而形成特征矢量。

[0376] 其中，此处注意在汉明距离的情况下是$b_i\in\{0,1\}$，在欧几里得平方距离的情况下是$b_i\in\{0,1,\cdots,q-1\}$。

[0377] 接下来，在步骤S1003中，随机数生成部203从0至q-1的整数中均匀随机地取出4T次值，设为$\{r_{2,i},r_{3,i},r\hat{}_{2,i},r\hat{}_{3,i}\}_{i=1,2,\cdots,T}$。

[0378] 接下来，在步骤S1004中，加密部204通过$c_i=b_iw_1+r_{2,i}w_2+r_{3,i}w_3$，$c\hat{}_i=b_iw\hat{}_1+r\hat{}_{2,i}w\hat{}_2+r\hat{}_{3,i}w\hat{}_3$，计算加密特征矢量$C=(c_1,c_2,\cdots,c_T)$、加密特征矢量$C\hat{}=(c\hat{}_1,c\hat{}_2,\cdots,c\hat{}_T)$。

[0379] 另外，w_1,w_2,w_3和$w\hat{}_1,w\hat{}_2,w\hat{}_3$是作为公开密钥的一部分(W以及W^)从解密装置103分发的。

[0380] 接下来，在步骤S1005中，通信部206将加密特征矢量$C=(c_1,c_2,\cdots,c_T)$、加密特征矢量$C\hat{}=(c\hat{}_1,c\hat{}_2,\cdots,c\hat{}_T)$发送到认证装置102。

[0381] 此时，期望使用例如SSL等通信用篡改检测技术来防止在通信的中途被篡改。

[0382] 最后，在步骤S1006中，认证装置102将加密特征矢量$C=(c_1,c_2,\cdots,c_T)$、加密特征矢量$C\hat{}=(c\hat{}_1,c\hat{}_2,\cdots,c\hat{}_T)$储存到存储部301中。

[0383] 接下来，使用图11、图12、图13，说明认证方法。

[0384] 另外，为了简化说明，此处说明另外通过ID信息等确定了在认证时成为认证的对象的用户的所谓1:1认证的情况。

[0385] 首先，在步骤S1101中，证明装置101的生物体信息抽出部201抽出用户的生物体信息。

[0386] 抽出方法与生物体信息的登记时相同。

[0387] 接下来，在步骤S1102中，证明装置101的特征矢量形成部202根据生物体信息，形成特征矢量$b'=(b'_1,b'_2,\cdots,b'_T)$。

[0388] 形成方法与生物体信息的登记时相同。

[0389] 其中，此处注意在汉明距离的情况下是$b'_i\in\{0,1\}$，在欧几里 得平方距离的情况下是$b'_i\in\{0,1,\cdots,q-1\}$。

[0390] 接下来，在步骤S1103中，证明装置101的随机数生成部203从0至q-1的整数中均匀随机地取出4T次值，设为$\{r'_{2,i},r'_{3,i},r\hat{}'_{2,i},r\hat{}'_{3,i}\}_{i=1,2,\cdots,T}$。

[0391] 接下来，在步骤S1104中，证明装置101的加密部204通过$c'_i=b'_iw_1+r'_{2,i}w_2+r'_{3,i}w_3$，$c\hat{}'_i=b'_iw\hat{}_1+r'_{2,i}w\hat{}_2+r'_{3,i}w\hat{}_3$，计算加密特征矢量$C'=(c'_1,c'_2,\cdots,c'_T)$、加密特征矢量$C\hat{}'=(c\hat{}'_1,c\hat{}'_2,\cdots,c\hat{}'_T)$。

[0392] 接下来，在步骤S1105中，证明装置101的通信部206将加密特征矢量$C'=(c'_1,c$

’2,…,c’T)、加密特征矢量C^’’=(c^’’1,c^’’2,…,c^’’T)发送到认证装置102。

[0393] 此时,期望使用例如SSL等通信用篡改检测技术来防止在通信的中途被篡改。

[0394] 接下来,在步骤S1106中,认证装置102的通信部206接收加密特征矢量C’=(c’1,c’2,…,c’T)、加密特征矢量C^’’=(c^’’1,c^’’2,…,c^’’T)。

[0395] 接下来,在步骤S1107中,认证装置102的加密类似度生成部302从存储部301取出加密特征矢量C=(c1,c2,…,cT)、加密特征矢量C^=(c^1,c^2,…,c^T)。

[0396] 此时,一般,在存储部301中储存有多个用户的加密生物体信息,但关于从其中取出哪个,使用另外提供的ID信息。

[0397] 接下来,在步骤S1108中,认证装置102的随机数生成部203从0至q-1的整数中均匀随机地取出6T次值,设为{s1,i,s2,i,s3,i,s^1,i,s^2,i,s^3,i}i=1,2,…,T。

[0398] 接下来,在步骤S1109中,认证装置102的随机数生成部203从0至q-1的整数中均匀随机地取出4次值,设为{u2,u3,u^2,u^3}。

[0399] 接下来,在步骤S1110中,认证装置102的加密类似度生成部302计算di=(ci-c’i)+s1,iW1+s2,iW2+s3,iW3。

[0400] 另外,w1、w2、w3是作为公开密钥的一部分(W)从解密装置 103分发的。

[0401] 接下来,在步骤S1111中,认证装置102的加密类似度生成部302计算d^i=(c^i-c^’i)+s^1,iw^1+s^2,iw^2+s^3,iw^3。

[0402] 另外,w^1、w^2、w^3是作为公开密钥的一部分(W^)从解密装置103分发的。

[0403] 接下来,在步骤S1112中,认证装置102的加密类似度生成部302依照式10,计算E。

[0404] 【式10】

[0405] $$E=\sum_{i=1}^{T}(\hat{s}_{1,i}(\mathbf{c}_i-\mathbf{c}_i')+s_{1,i}\hat{s}_{1,i}\mathbf{w}_1)+u_2\mathbf{w}_2+u_3\mathbf{w}_3$$

[0406] 接下来,在步骤S1113中,认证装置102的加密类似度生成部302依照式11,计算E^。

[0407] 【式11】

[0408] $$\hat{E}=\sum_{i=1}^{T}s_{1,i}(\hat{\mathbf{c}}_i-\hat{\mathbf{c}}_i')+\hat{u}_2\hat{\mathbf{w}}_2+\hat{u}_3\hat{\mathbf{w}}_3$$

[0409] 接下来,在步骤S1114中,认证装置102的通信部206将(d1,…,dT,d^1,…,d^T…,E,E^)发送到解密装置103。

[0410] 此时,期望使用例如SSL等通信用篡改检测技术来防止在通信的中途被篡改。

[0411] 在本实施方式中,(d1,…,dT,d^1,…,d^T…,E,E^)成为加密类似度信息的例子。

[0412] 接下来,在步骤S715中,解密装置103的通信部404接收(d1,…,dT,d^1,…,d^T,E,E^)。

[0413] 接下来,在步骤S716中,解密装置103的解密部402从存储部403取出秘密密钥sk=(X,X^)。

[0414] 接下来,在步骤S717中,解密装置103的解密部402计算X的逆矩阵X^{-1}=(ti,j)以及X^的逆矩阵$X\hat{}^{-1}$=(t^i,j)。

[0415] 另外,该值并非每次计算,也可以以预先计算了的状态储存到存 储部403中,并将其取出。

[0416] 接下来,在步骤S718中,解密装置103依照式12计算Z1。

[0417] 【式12】

[0418] $$Z_1=\prod_{i=1}^{T} e(Deco(\mathbf{d}_i,\langle \mathbf{w}_1\rangle,X),Deco(\hat{\mathbf{d}}_i,\langle \hat{\mathbf{w}}_1\rangle,\hat{X}))$$

[0419] 此处，Deco算法是如以下的式13那样计算的。另外，式13中的k是整数。

[0420] 【式13】

[0421] Deco(d_i,<w_1>,X)：

[0422] $$\mathbf{y}=\sum_{i=1}^{3}\sum_{k=1}^{3} t_{i,1}x_{1,k}\phi_{k,i}(\mathbf{d}_i)$$

[0423] $$\mathbf{Deco}\ (\ \hat{\mathbf{d}}_i,<\hat{\mathbf{w}}_1>,\hat{X}\ )\ :$$

[0424] $$\hat{\mathbf{y}}=\sum_{i=1}^{3}\sum_{k=1}^{3} \hat{t}_{i,1}\hat{x}_{1,k}\phi_{k,i}(\hat{\mathbf{d}}_i)$$

[0425] 接下来，在步骤S719中，解密装置103的解密部402计算Z_2=e(Deco(E,<w_1>,X),w^$_1$)·e(w_1,Deco(E^,<w^$_1$>,X^))。

[0426] 该Deco算法也是与上述同样地计算的。

[0427] 接下来，在步骤S720中，解密装置103的解密部402计算$Z=Z_1/Z_2$。

[0428] 接下来，在步骤S721中，解密装置103的解密部402计算以e(g,g^)为底的Z的离散对数d。另外，e(g,g^)是作为公开密钥的一部分从解密装置103分发的。

[0429] 该离散对数d对应于特征点的一致数，表示类似度。

[0430] 另外，求出离散对数的计算在现代的计算机能力上是困难的，但在d小的情况下，能够高效地计算。

[0431] 在本实施方式中，d比位数q充分小，所以能够高效地计算。

[0432] 接下来，在步骤S722中，解密装置103的通信部404将类似度 d发送到认证装置102。

[0433] 此时，期望使用例如SSL等通信用篡改检测技术来防止在通信的中途被篡改。

[0434] 接下来，在步骤S723中，认证装置102的通信部304接收类似度d。

[0435] 接下来，在步骤S724中，判定类似度d是否为阈值以上。

[0436] 阈值是考虑所利用的生物体信息的种类、安全性要件等各种要素而预先在系统中决定的值。

[0437] 如果是阈值以上，则判断为从证明装置101送来的加密生物体信息是用ID指定了的本人的信息。

[0438] 另一方面，如果小于阈值，则判断为从证明装置101送来的加密生物体信息并非用ID指定了的人物的信息，而是他人的信息。

[0439] 通过以上的步骤，认证装置102能够在与证明装置101之间进行生物体认证。

[0440] 另外，在本实施方式中，公开了使用三维的双对配对矢量空间的方法，但三维仅为例示，无需一定是三维。

[0441] 例如，在二维中也能够实施，在四维以上中也能够实施。

[0442] 在二维的情况下，去掉在本实施方式中出现的w_3,w^$_3$的矢量来实施即可。

[0443] 由此，具有能够降低生物体信息的登记时、认证时的计算量这样的效果。

[0444] 另外，在四维以上的情况下，使增加了的量的矢量发挥与w_2，w_3，$w\hat{}_2$，$w\hat{}_3$同样的作用即可。

[0445] 即，在计算c_i，$c\hat{}_i$，d_i，$d\hat{}_i$时，对增加了的量的矢量乘以随机数系数，相加到w_2，w_3，$w\hat{}_2$，$w\hat{}_3$即可。

[0446] 由此，能够制作破译更困难的密文，能够提高安全性。

[0447] 实施方式6.

[0448] 在实施方式6中，为了补充实施方式2以及实施方式4的说明，说明专利文献1的实施方式4记载的方式中的设置处理、登记处理、认证处理。

[0449] 另外，在本实施方式中，设置处理、登记处理、认证处理的概要也如图19-22所示。

[0450] 在专利文献1的实施方式4记载的方式中，以如下认证方式为例子进行说明：作为在生物体认证中使用的特征矢量，准备特征点的数组，在用户保有该特征点的情况下将1储存到数组中，在不保有特征点的情况下将0储存到数组中，将数组作为特征矢量，在认证时将1一致的部位的数量作为类似度的指标。

[0451] 首先，使用图14来说明设置。

[0452] 图14是示出参数生成部401中的公开密钥以及秘密密钥的生成步骤的流程图。

[0453] 首先，在步骤S1301中，参数生成部401决定素数p，q、群G，G_T。

[0454] 另外，素数根据保密等级确定，为了使素数p与q之积成为群位数，通常以无法进行素因数分解的方式，将素数设为1024比特、2048比特等大的规模的素数。

[0455] 接下来，在步骤S1302中，参数生成部401从G均匀随机地选择g、u，计算$h=u^q$。

[0456] 最后，在步骤S1303中，参数生成部401公开公开密钥$pk=((G,G_T,N,e),g,h,e(g,g))$，将秘密密钥$sk=p$储存到存储部403中。

[0457] 接下来，使用图15，说明生物体信息的登记方法。

[0458] 另外，此处，说明用户经由证明装置101向认证装置102登记生物体信息的情况，但在认证装置102上直接登记生物体信息的情况、经由登记用的专用装置登记的情况下等，也能够通过同样的步骤实现。

[0459] 图15是示出在证明装置101中登记生物体信息的步骤的流程图。

[0460] 首先，在步骤S1401中，生物体信息抽出部201抽出用户的生物体信息。其中有各种方法，例如通过对指纹照射光并用传感器读取指 纹型来抽出。

[0461] 接下来，在步骤S1402中，特征矢量形成部202根据生物体信息，形成特征矢量$b=(b_1,b_2,\cdots,b_T)$。

[0462] 接下来，在步骤S1403中，随机数生成部203从0至N-1的整数中均匀随机地取出T次值，设为$\{r_i\}_{i=1,2,\cdots,T}$。

[0463] 接下来，在步骤S1404中，加密部204通过$c_i=g^{b_i}h^{r_i}$，计算加密特征矢量$C=(c_1,c_2,\cdots,c_T)$。

[0464] 另外，g、h是作为公开密钥的一部分从解密装置103分发的。

[0465] 接下来，在步骤S1405中，通信部206将加密特征矢量$C=(c_1,c_2,\cdots,c_T)$发送到认证装置102。

[0466] 最后，在步骤S1406中，认证装置102将加密特征矢量$C=(c_1,c_2,\cdots,c_T)$储存到存储部301中。

[0467] 接下来，使用图16、图17、图18，说明认证方法。

[0468] 另外，为了简化说明，此处，说明另外通过ID信息等确定了在认证时成为认证的对象的用户的所谓1:1认证的情况。

[0469] 首先，在步骤S1801中，证明装置101的生物体信息抽出部201抽出用户的生物体信息。

[0470] 抽出方法与生物体信息的登记时相同。

[0471] 接下来，在步骤S1802中，证明装置101的特征矢量形成部202根据生物体信息，形成特征矢量$b'=(b'_1,b'_2,\cdots,b'_T)$。

[0472] 形成方法与生物体信息的登记时相同。

[0473] 接下来，在步骤S1803中，证明装置101的随机数生成部203从0至N-1的整数中均匀随机地取出T次值，设为$\{r'_i\}_{i=1,2,\cdots,T}$。

[0474] 接下来，在步骤S1804中，证明装置101的加密部204通过$c'_i=g^{b'_i}h^{r'_i}$，计算加密特征矢量$C'=(c'_1,c'_2,\cdots,c'_T)$。

[0475] 接下来，在步骤S1805中，证明装置101的通信部206将加密特征矢量$C'=(c'_1,c'_2,\cdots,c'_T)$发送到认证装置102。

[0476] 此时，期望使用例如SSL等通信用篡改检测技术来防止在通信的中途被篡改。

[0477] 接下来，在步骤S1806中，认证装置102的通信部206接收加密特征矢量$C'=(c'_1,c'_2,\cdots,c'_T)$。

[0478] 接下来，在步骤S1807中，认证装置102的加密类似度生成部302从存储部301取出加密特征矢量$C=(c_1,c_2,\cdots,c_T)$。

[0479] 接下来，在步骤S1808中，认证装置102的随机数生成部305从0至N-1的整数中均匀随机地取出值，设为s。

[0480] 在步骤S1809中，认证装置102的加密类似度生成部302依照式14，计算E。

[0481] 【式14】

[0482] $$E=\prod_{i=1}^{T}e(c_i,g)\cdot e(c'_i,g)\cdot e(c_i,c'_i)^{-2}\cdot e(g,h)^{s}$$

[0483] 接下来，在步骤S1810中，认证装置102的通信部304将E发送到解密装置103。

[0484] 此时，期望使用例如SSL等通信用篡改检测技术来防止在通信的中途被篡改。

[0485] 在本实施方式中，E成为加密类似度信息。

[0486] 接下来，在步骤S1811中，解密装置103的通信部404接收E。

[0487] 接下来，在步骤S1812中，解密装置103的解密部402从存储部403取出秘密密钥p。

[0488] 接下来，在步骤S1813中，解密装置103的解密部402计算$Z=E^p$。

[0489] 接下来，在步骤S1814中，解密装置103的解密部402计算以$e(g,g)^p$为底的Z的离散对数d。

[0490] 另外，e(g,g)是作为公开密钥的一部分从解密装置103分发的。

[0491] 在本实施方式中，该离散对数d也相当于类似度。

[0492] 接下来，在步骤S1815中，解密装置103的通信部404将d发送到认证装置102。此时，期望使用例如SSL等通信用篡改检测技术来防止在通信的中途被篡改。

[0493] 接下来，在步骤S1816中，认证装置102的通信部304接收类似度d。

[0494] 接下来，在步骤S1817中，判定部303判定类似度d是否为阈值以上。

[0495] 该阈值是考虑所利用的生物体信息的种类、安全性要件等各种要素而预先在系统中决定的值。

[0496] 如果是阈值以上，则判断为从证明装置101送来的加密生物体信息是用ID指定了的本人的信息。

[0497] 另一方面，如果小于阈值，则判断为从证明装置101送来的加密生物体信息并非用ID指定了的人物的信息，而是他人的信息。

[0498] 通过以上的步骤，认证装置102能够在与证明装置101之间进行生物体认证。

[0499] 最后，说明实施方式1-6所示的证明装置101、认证装置102、解密装置103的硬件结构例。

[0500] 图23是示出实施方式1-6所示的证明装置101、认证装置102、解密装置103的硬件资源的一个例子的图。

[0501] 另外，图23的结构仅为证明装置101、认证装置102、解密装置103的硬件结构的一个例子，证明装置101、认证装置102、解密装置103的硬件结构不限于图23记载的结构，也可以是其他结构。

[0502] 在图23中，证明装置101、认证装置102、解密装置103具备执行程序的CPU911(Central Processing Unit、还称为中央处理装置、处理装置、运算装置、微处理器、微型计算机、处理器)。

[0503] CPU911经由总线912，例如与ROM(Read Only Memory，只读存储器)913、RAM(Random Access Memory，随机访问存储器)914、通信板915、显示装置901、键盘902、鼠标903、磁盘装置920连接，控制这些硬件设备。

[0504] 进而，CPU911也可以与FDD904(Flexible Disk Drive，软盘驱动器)、高密度盘装置905(CDD)、打印机装置906连接。另外，证明装置101与用于读取生物体信息的读取装置907连接。另外，也 可以代替磁盘装置920，而使用光盘装置、存储卡(注册商标)读写装置等存储装置。

[0505] RAM914是易失性存储器的一个例子。ROM913、FDD904、CDD905、磁盘装置920的存储介质是非易失性存储器的一个例子。它们是存储装置的一个例子。

[0506] 在实施方式1-6中说明了的“存储部”通过RAM914、磁盘装置920等实现。

[0507] 通信板915、键盘902、鼠标903、读取装置907、FDD904等是输入装置的一个例子。

[0508] 另外，通信板915、显示装置901、打印机装置906等是输出装置的一个例子。

[0509] 通信板915除了与其他装置连接以外，例如，也可以与LAN(局域网)、因特网、WAN(广域网)、SAN(存储区域网络)等连接。

[0510] 在磁盘装置920中，存储了操作系统921(OS)、视窗系统922、程序群923、文件群924。

[0511] CPU911在利用操作系统921、视窗系统922的同时，执行程序群923的程序。

[0512] 另外，在RAM914中，临时地储存使CPU911执行的操作系统921的程序、应用程序的至少一部分。

[0513] 另外，在RAM914中，储存由CPU911实施的处理所需的各种数据。

[0514] 另外，在ROM913中，储存了BIOS(Basic Input Output System，基本输入输出系

统)程序,在磁盘装置920中储存了引导程序。

[0515] 在证明装置101、认证装置102、解密装置103的起动时,执行ROM913的BIOS程序以及磁盘装置920的引导程序,通过BIOS程序以及引导程序,起动操作系统921。

[0516] 在上述程序群923中,存储了执行在实施方式1-6的说明中说明为“～部”(除了“存储部”以外,以下同样)的功能的程序。程序由CPU911读出并执行。

[0517] 在文件群924中,将表示在实施方式1-6的说明中说明为“～的判断”、“～的判定”、“～的生成”、“～的计算”、“～的比较”、“～的导出”、“～的抽出”、“～的形成”、“～的更新”、“～的设定”、“～的登记”、“～的选择”等的处理的结果的信息、数据、信号值、变量值、参数存储为“～文件”、“～数据库”的各项目。

[0518] “～文件”、“～数据库”存储于盘、存储器等记录介质中。关于在盘、存储器等存储介质中存储了的信息、数据、信号值、变量值、参数,经由读写电路,通过CPU911读出到主存储器、高速缓存存储器中,用于抽出、检索、参照、比较、运算、计算、处理、编辑、输出、印刷、显示等CPU的动作。

[0519] 在抽出、检索、参照、比较、运算、计算、处理、编辑、输出、印刷、显示的CPU的动作的期间,信息、数据、信号值、变量值、参数被临时存储到主存储器、寄存器、高速缓存存储器、缓冲存储器等中。

[0520] 另外,在实施方式1-6中说明的流程图的箭头的部分主要表示数据、信号的输入输出,数据、信号值记录于RAM914的存储器、FDD904的软盘、CDD905的高密度盘、磁盘装置920的磁盘、其他光盘、迷你盘、DVD等记录介质中。另外,数据、信号通过总线912、信号线、电缆、其他传送介质在线传送。

[0521] 另外,在实施方式1-6的说明中说明为“～部”的部分既可以是“～电路”、“～装置”、“～设备”,并且也可以是“～步骤”、“～工序”、“～处理”。

[0522] 即,能够通过在实施方式1-6中说明的流程图所示的步骤、工序、处理,实现本发明的“数据处理方法”。

[0523] 另外,说明为“～部”的部分也可以通过在ROM913中存储了的固件实现。或者,也可以仅通过软件、或者仅通过元件、设备、基板、布线等硬件、或者通过软件和硬件的组合、进而通过与固件的组合来实施。将固件和软件作为程序存储到磁盘、软盘、光盘、高密度盘、迷你盘、DVD等记录介质中。程序由CPU911读出并由CPU911执 行。即,程序使计算机作为实施方式1-6的“～部”发挥功能。或者,使计算机执行实施方式1-6的“～部”的步骤、方法。

[0524] 这样,实施方式1-6所示的证明装置101、认证装置102、解密装置103是具备作为处理装置的CPU、作为存储装置的存储器、磁盘等、作为输入装置的键盘、鼠标、通信板等、作为输出装置的显示装置、通信板等的计算机,使用这些处理装置、存储装置、输入装置、输出装置来实现如上所述表示为“～部”的功能。

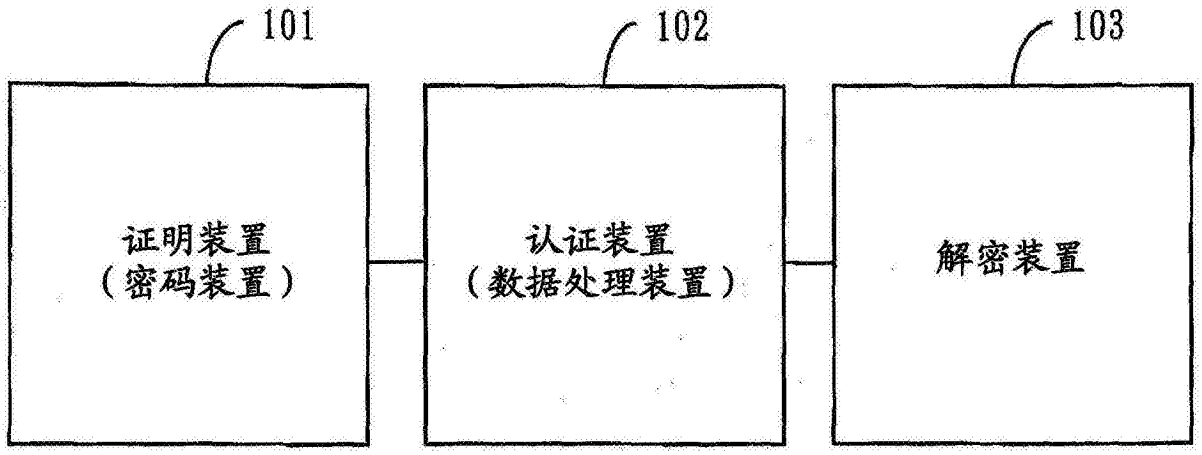

101
102
103
证明装置
（密码装置）
认证装置
（数据处理装置）
解密装置

图1

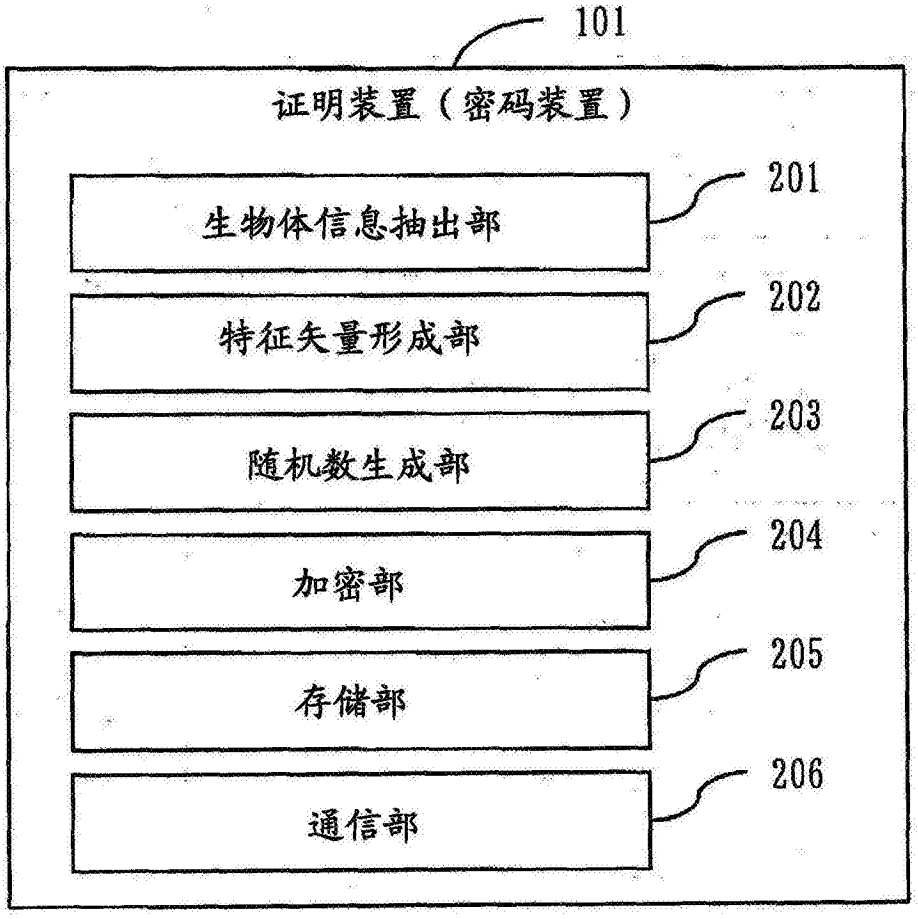

101
证明装置（密码装置）
生物体信息抽出部
201
特征矢量形成部
202
随机数生成部
203
加密部
204
存储部
205
通信部
206

图2

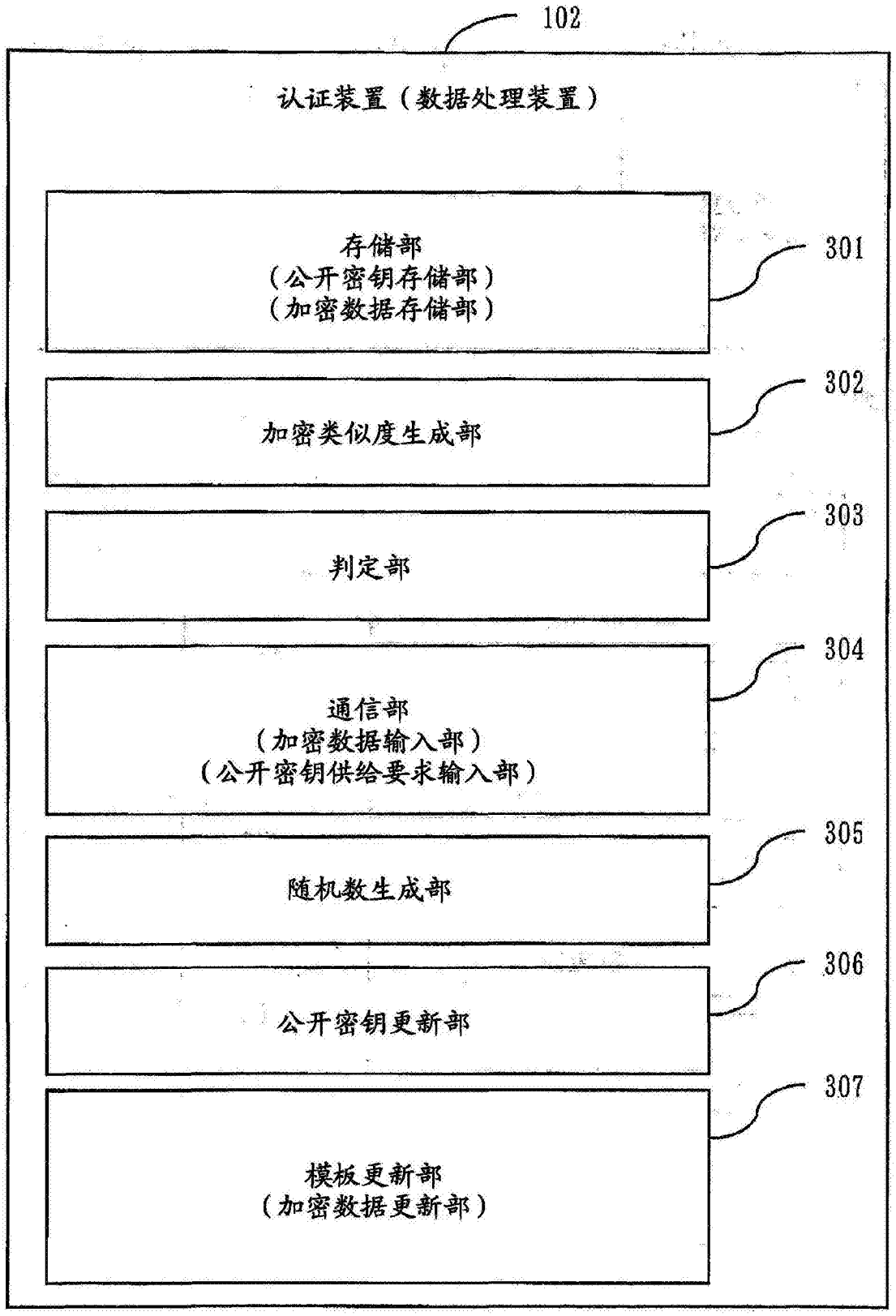

102
认证装置（数据处理装置）
存储部
（公开密钥存储部）
（加密数据存储部）
301
加密类似度生成部
302
判定部
303
通信部
（加密数据输入部）
（公开密钥供给要求输入部）
304
随机数生成部
305
公开密钥更新部
306
模板更新部
（加密数据更新部）
307

图3

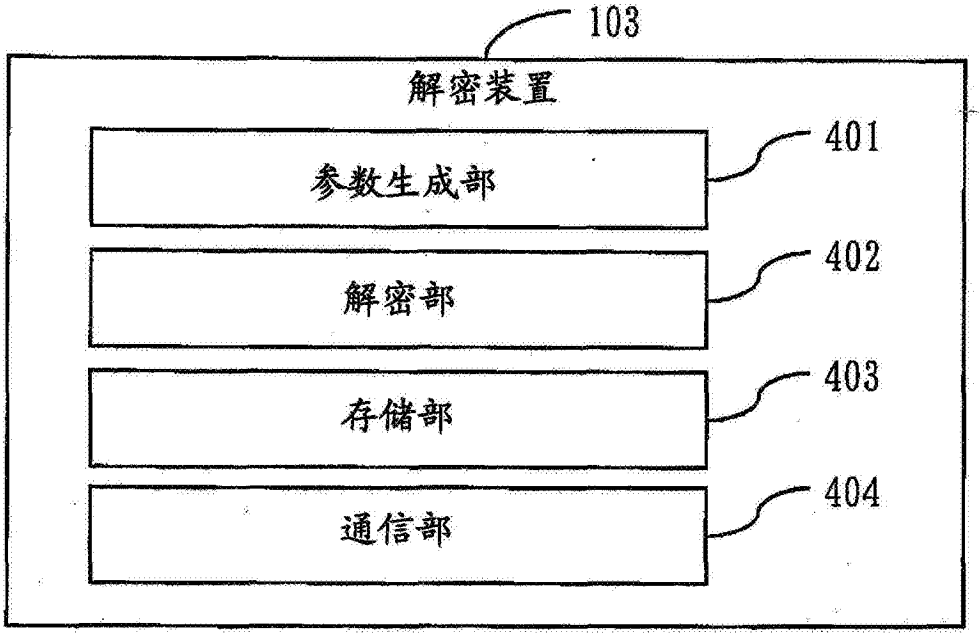


图4

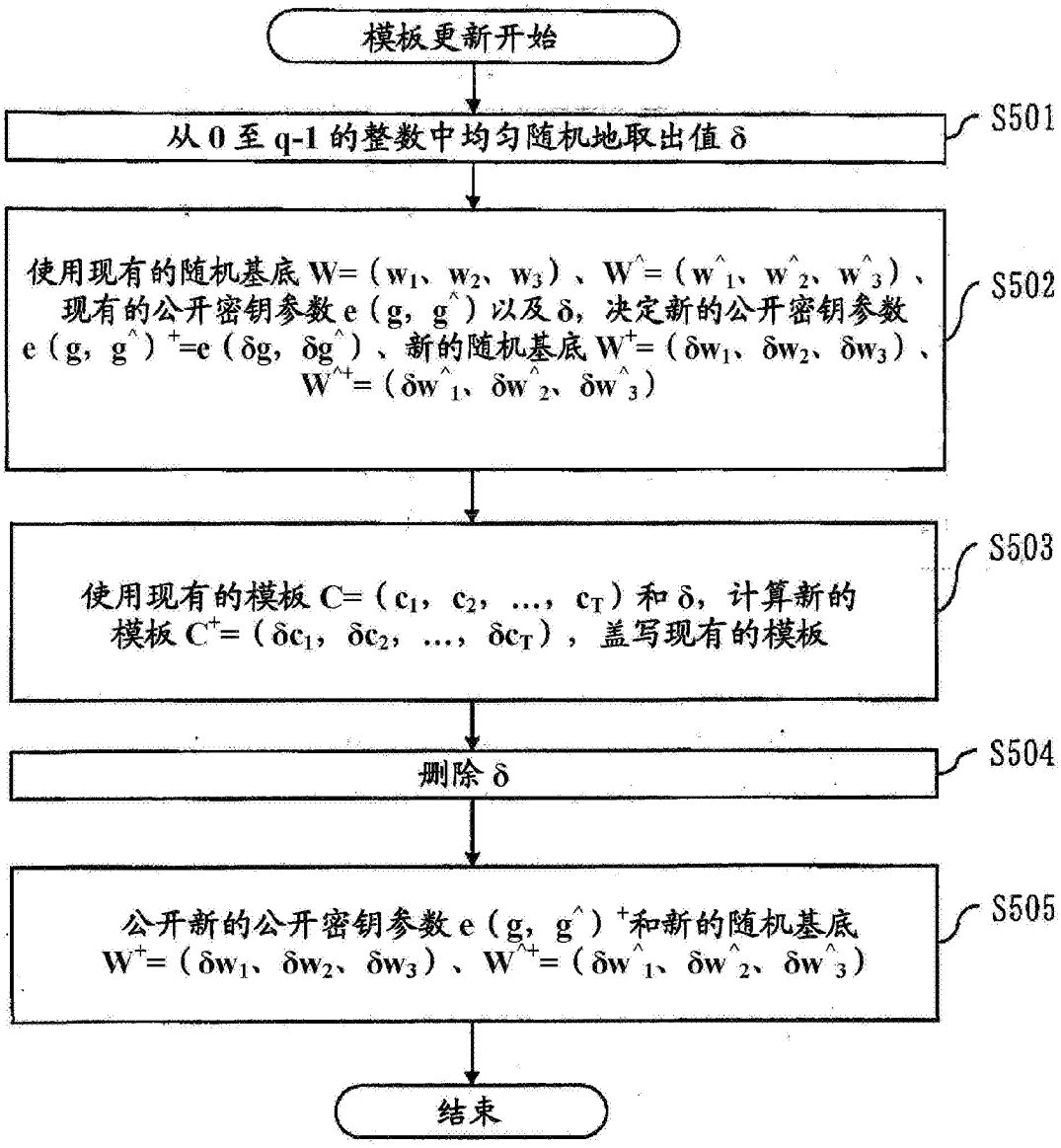

模板更新开始
从 0 至 q-1 的整数中均匀随机地取出值 δ
S501
使用现有的随机基底 W=（w1、w2、w3）、W^=（w^1、w^2、w^3）、现有的公开密钥参数 e（g，g^）以及 δ，决定新的公开密钥参数 e（g，g^）+=e（δg，δg^）、新的随机基底 W+=（δw1、δw2、δw3）、W^+=（δw^1、δw^2、δw^3）
S502
使用现有的模板 C=（c1，c2，…，cT）和 δ，计算新的模板 C+=（δc1，δc2，…，δcT），盖写现有的模板
S503
删除 δ
S504
公开新的公开密钥参数 e（g，g^）+和新的随机基底 W+=（δw1、δw2、δw3）、W^+=（δw^1、δw^2、δw^3）
S505
结束

图5

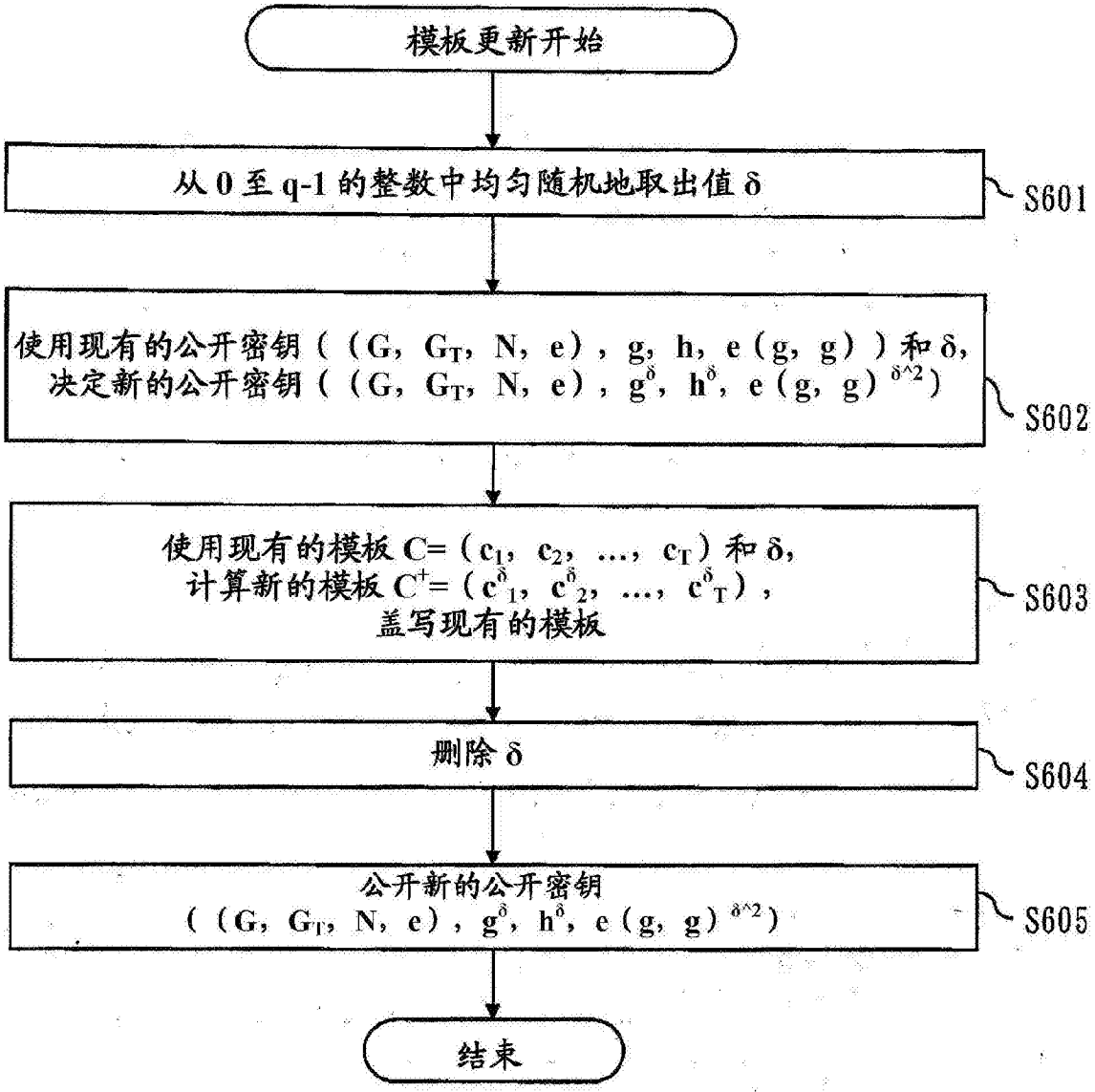

模板更新开始
从 0 至 q-1 的整数中均匀随机地取出值 δ
S601
使用现有的公开密钥（（G，G_T，N，e），g，h，e（g，g））和 δ，
决定新的公开密钥（（G，G_T，N，e），g^{δ}，h^{δ}，e（g，g）$^{\delta^2}$）
S602
使用现有的模板 C=（c_1，c_2，…，c_T）和 δ，
计算新的模板 C^+=（c^{δ}_1，c^{δ}_2，…，c^{δ}_T），
盖写现有的模板
S603
删除 δ
S604
公开新的公开密钥
（（G，G_T，N，e），g^{δ}，h^{δ}，e（g，g）$^{\delta^2}$）
S605
结束

图6

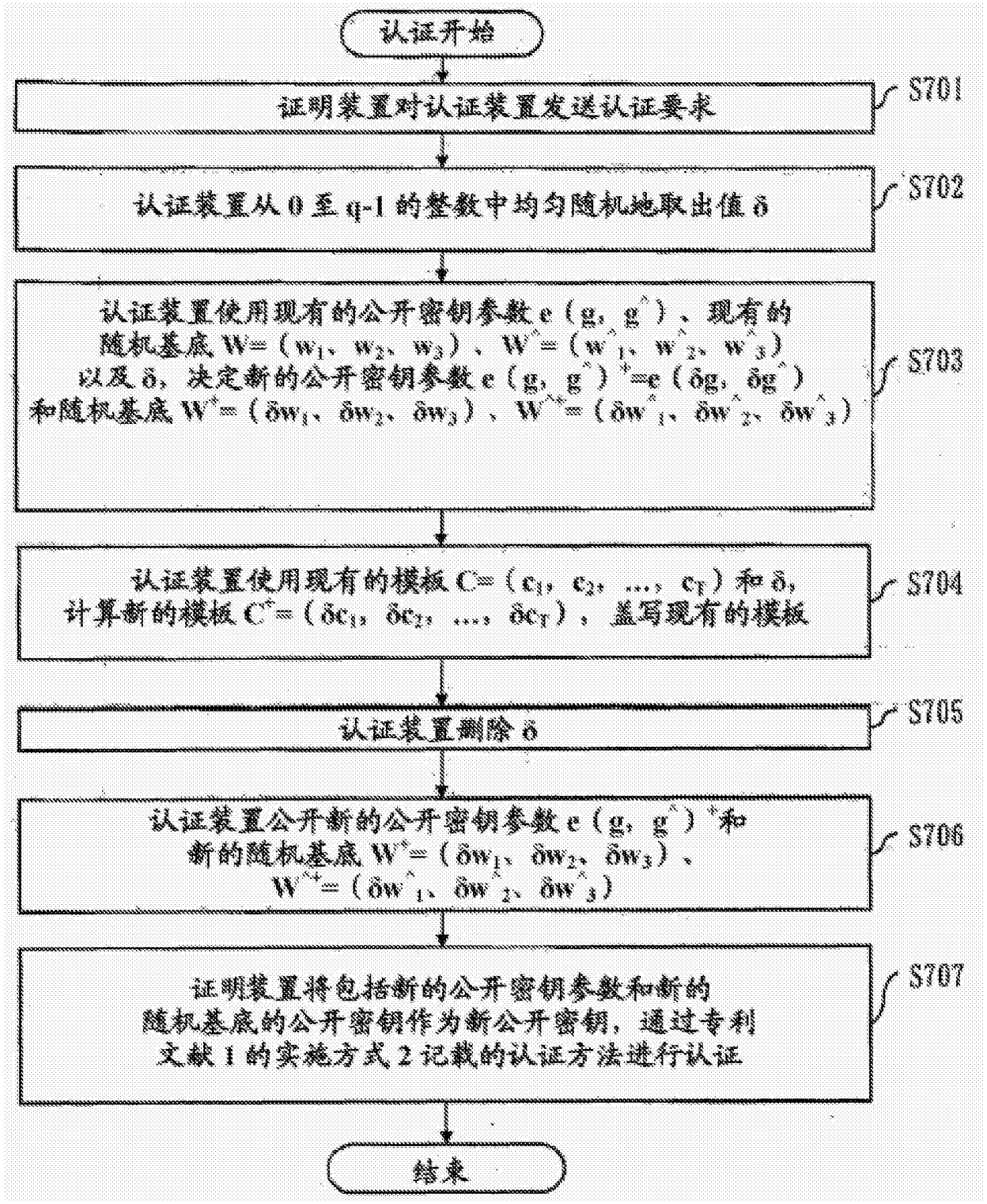

认证开始
证明装置对认证装置发送认证要求
S701
认证装置从 0 至 q-1 的整数中均匀随机地取出值 δ
S702
认证装置使用现有的公开密钥参数 e (g, g^) 、现有的随机基底 W=(w1、w2、w3) 、W^=(w^1、w^2、w^3) 以及 δ，决定新的公开密钥参数 e (g, g^)*=e (δg, δg^) 和随机基底 W*=(δw1、δw2、δw3) 、W^*=(δw^1、δw^2、δw^3)
S703
认证装置使用现有的模板 C=(c1, c2, ..., cT) 和 δ，计算新的模板 C*=(δc1, δc2, ..., δcT) ，盖写现有的模板
S704
认证装置删除 δ
S705
认证装置公开新的公开密钥参数 e (g, g^)* 和新的随机基底 W*=(δw1、δw2、δw3) 、W^*=(δw^1、δw^2、δw^3)
S706
证明装置将包括新的公开密钥参数和新的随机基底的公开密钥作为新公开密钥，通过专利文献 1 的实施方式 2 记载的认证方法进行认证
S707
结束

图7

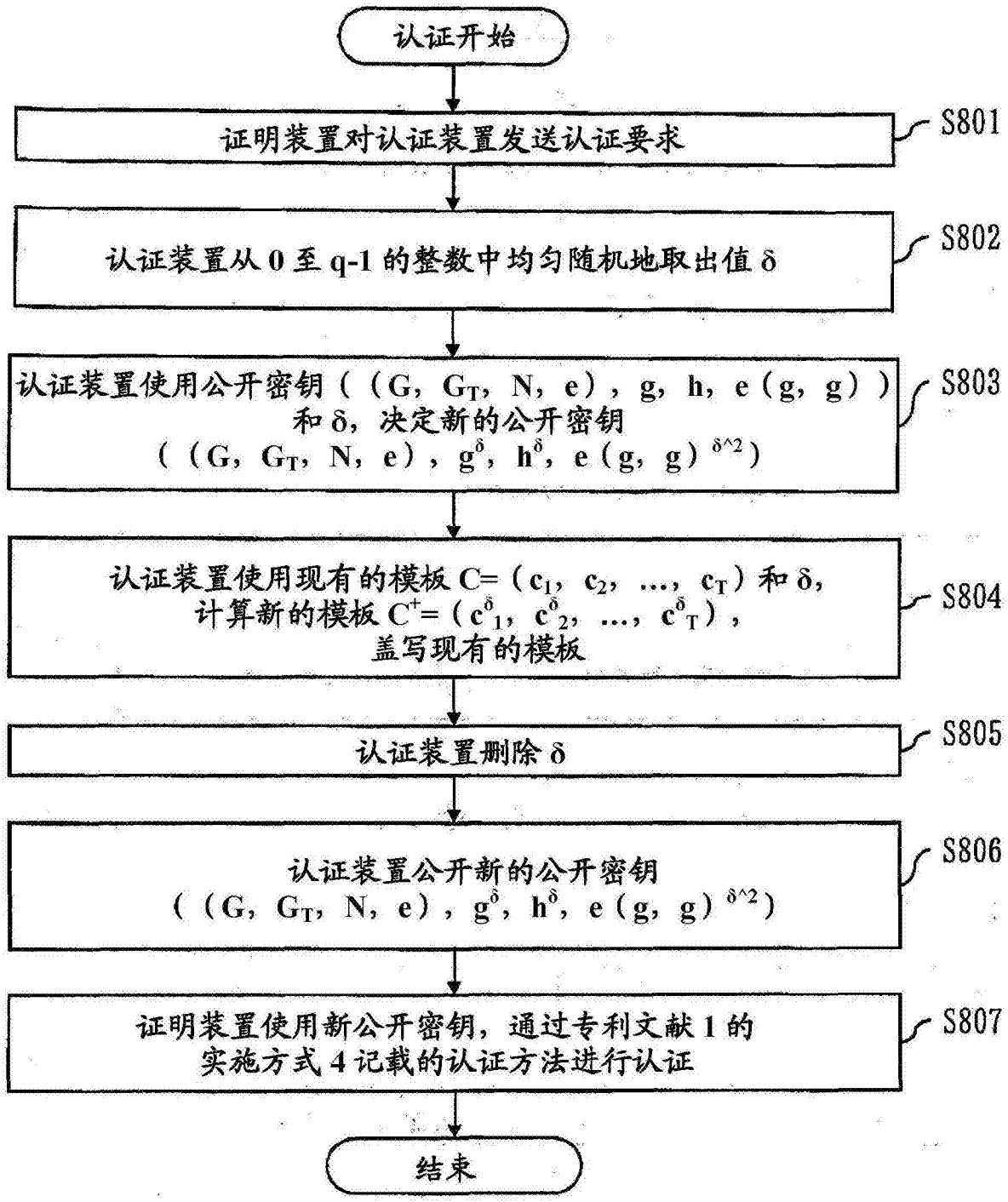

认证开始
证明装置对认证装置发送认证要求
S801
认证装置从 0 至 q-1 的整数中均匀随机地取出值 δ
S802
认证装置使用公开密钥（（G，G_T，N，e），g，h，e（g，g））和 δ，决定新的公开密钥（（G，G_T，N，e），g^{δ}，h^{δ}，$e(g,g)^{\delta^2}$）
S803
认证装置使用现有的模板 C=（c_1，c_2，…，c_T）和 δ，计算新的模板 C^{+}=（c^{δ}_1，c^{δ}_2，…，c^{δ}_T），盖写现有的模板
S804
认证装置删除 δ
S805
认证装置公开新的公开密钥（（G，G_T，N，e），g^{δ}，h^{δ}，$e(g,g)^{\delta^2}$）
S806
证明装置使用新公开密钥，通过专利文献 1 的实施方式 4 记载的认证方法进行认证
S807
结束

图8

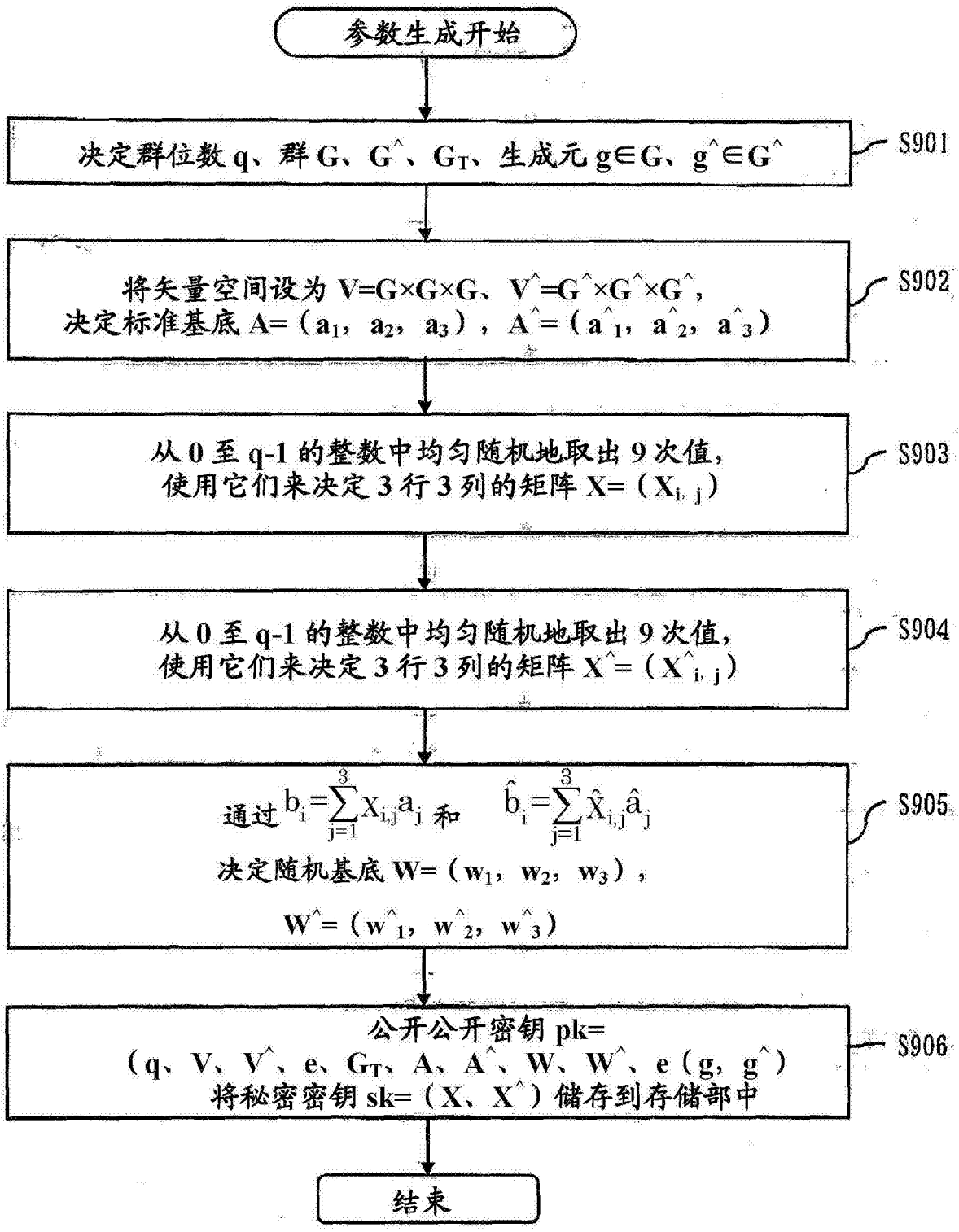

参数生成开始
决定群位数 q、群 G、$\hat{G}$、G_T、生成元 $g \in G$、$\hat{g} \in \hat{G}$
S901
将矢量空间设为 $V=G\times G\times G$、$\hat{V}=\hat{G}\times\hat{G}\times\hat{G}$，
决定标准基底 $A=(a_1, a_2, a_3)$，$\hat{A}=(\hat{a}_1, \hat{a}_2, \hat{a}_3)$
S902
从 0 至 q-1 的整数中均匀随机地取出 9 次值，
使用它们来决定 3 行 3 列的矩阵 $X=(X_{i,j})$
S903
从 0 至 q-1 的整数中均匀随机地取出 9 次值，
使用它们来决定 3 行 3 列的矩阵 $\hat{X}=(\hat{X}_{i,j})$
S904
通过 $b_i=\sum_{j=1}^{3} X_{i,j}a_j$ 和 $\hat{b}_i=\sum_{j=1}^{3} \hat{X}_{i,j}\hat{a}_j$
决定随机基底 $W=(w_1, w_2, w_3)$，
$\hat{W}=(\hat{w}_1, \hat{w}_2, \hat{w}_3)$
S905
公开公开密钥 pk=
$(q, V, \hat{V}, e, G_T, A, \hat{A}, W, \hat{W}, e(g, \hat{g}))$
将秘密密钥 $sk=(X, \hat{X})$ 储存到存储部中
S906
结束

图9

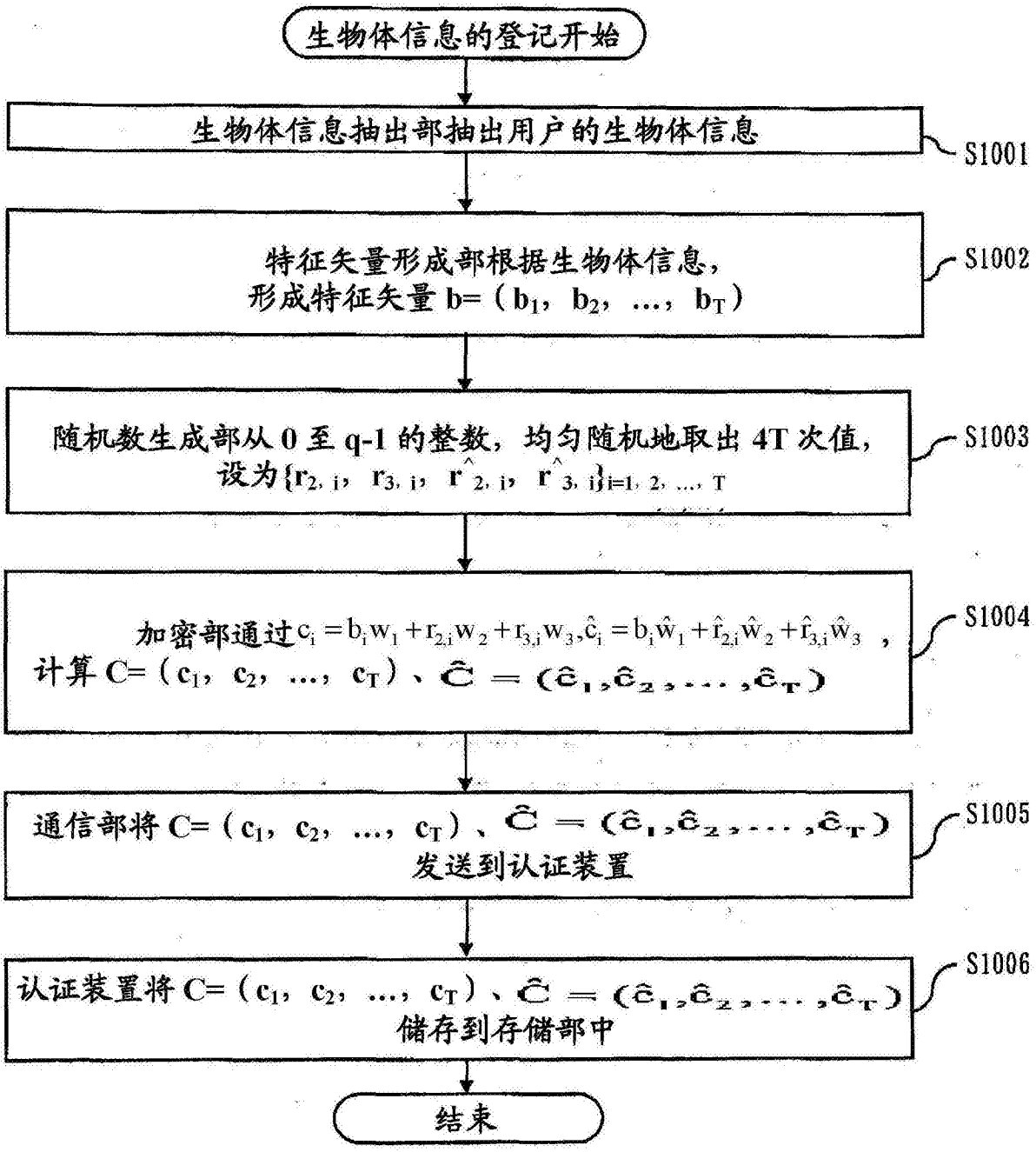

生物体信息的登记开始
生物体信息抽出部抽出用户的生物体信息
S1001
特征矢量形成部根据生物体信息，
形成特征矢量 b=（b1，b2，…，bT）
S1002
随机数生成部从 0 至 q-1 的整数，均匀随机地取出 4T 次值，
设为{r2, i，r3, i，r^2, i，r^3, i}i=1, 2, …, T
S1003
加密部通过 $c_i = b_i w_1 + r_{2,i} w_2 + r_{3,i} w_3, \hat{c}_i = b_i \hat{w}_1 + \hat{r}_{2,i} \hat{w}_2 + \hat{r}_{3,i} \hat{w}_3$ ，
计算 C=（c1，c2，…，cT）、$\hat{C} = (\hat{c}_1, \hat{c}_2, \ldots, \hat{c}_T)$
S1004
通信部将 C=（c1，c2，…，cT）、$\hat{C} = (\hat{c}_1, \hat{c}_2, \ldots, \hat{c}_T)$
发送到认证装置
S1005
认证装置将 C=（c1，c2，…，cT）、$\hat{C} = (\hat{c}_1, \hat{c}_2, \ldots, \hat{c}_T)$
储存到存储部中
S1006
结束

图10

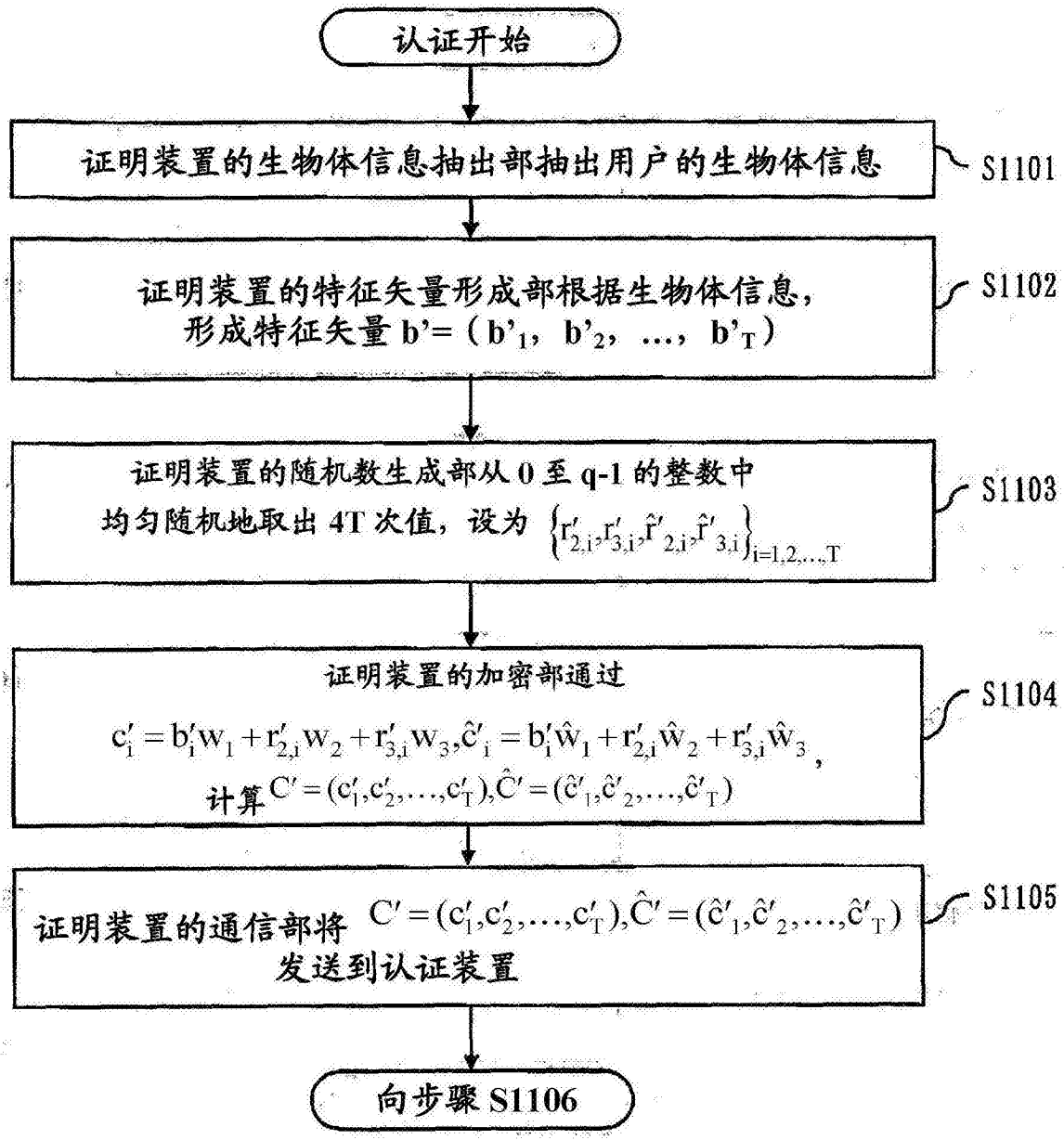

认证开始
证明装置的生物体信息抽出部抽出用户的生物体信息
S1101
证明装置的特征矢量形成部根据生物体信息，
形成特征矢量 b'=（b'1，b'2，…，b'T）
S1102
证明装置的随机数生成部从 0 至 q-1 的整数中
均匀随机地取出 4T 次值，设为 $\{r'_{2,i}, r'_{3,i}, \hat{r}'_{2,i}, \hat{r}'_{3,i}\}_{i=1,2,\ldots,T}$
S1103
证明装置的加密部通过
$c'_i = b'_i w_1 + r'_{2,i} w_2 + r'_{3,i} w_3, \hat{c}'_i = b'_i \hat{w}_1 + r'_{2,i} \hat{w}_2 + r'_{3,i} \hat{w}_3$，
计算 $C' = (c'_1, c'_2, \ldots, c'_T), \hat{C}' = (\hat{c}'_1, \hat{c}'_2, \ldots, \hat{c}'_T)$
S1104
证明装置的通信部将 $C' = (c'_1, c'_2, \ldots, c'_T), \hat{C}' = (\hat{c}'_1, \hat{c}'_2, \ldots, \hat{c}'_T)$
发送到认证装置
S1105
向步骤 S1106

图11

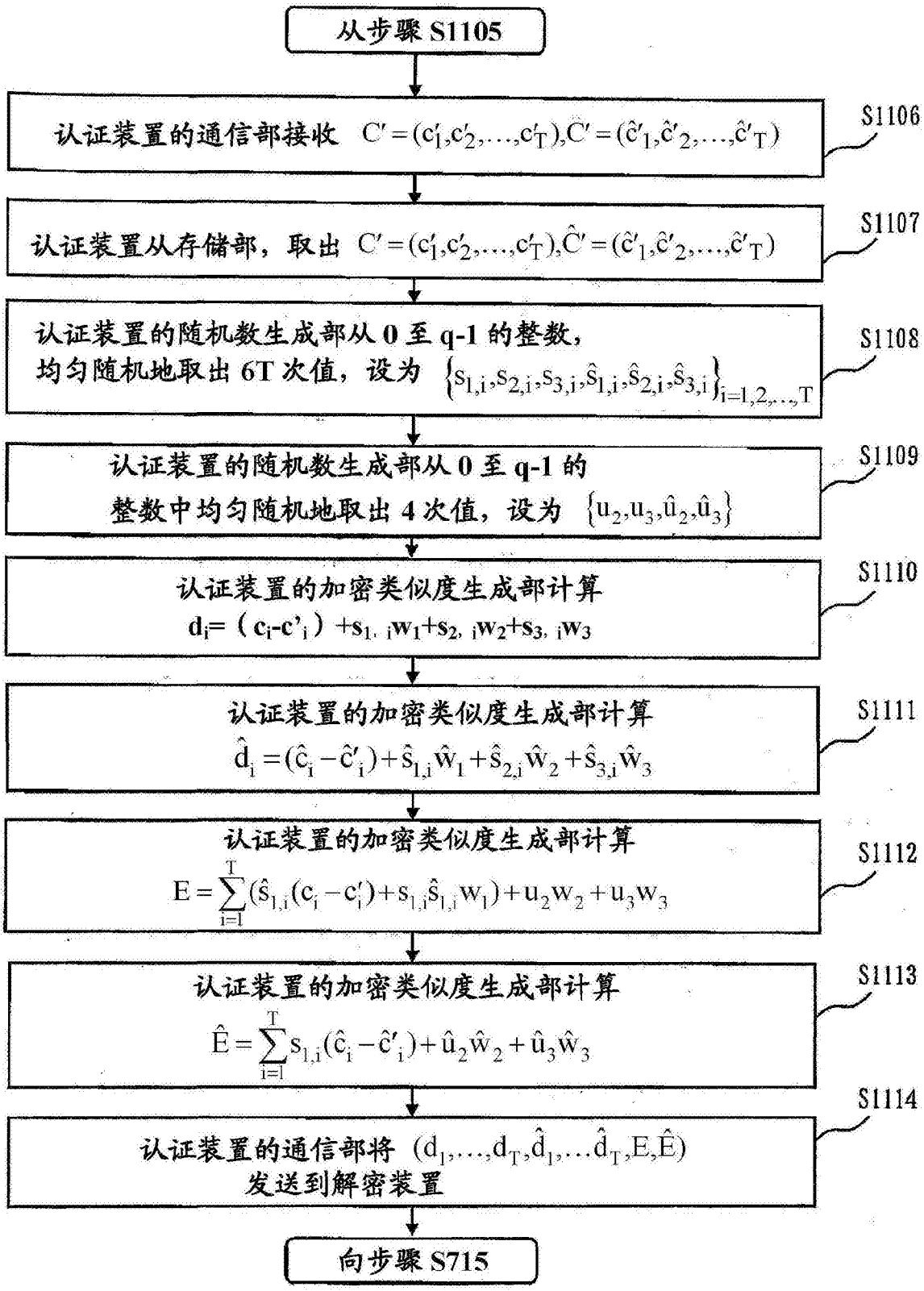

从步骤 S1105
认证装置的通信部接收 $C'=(c'_1,c'_2,\ldots,c'_T),\hat{C}'=(\hat{c}'_1,\hat{c}'_2,\ldots,\hat{c}'_T)$
S1106
认证装置从存储部，取出 $C'=(c'_1,c'_2,\ldots,c'_T),\hat{C}'=(\hat{c}'_1,\hat{c}'_2,\ldots,\hat{c}'_T)$
S1107
认证装置的随机数生成部从 0 至 q-1 的整数，
均匀随机地取出 6T 次值，设为 $\{s_{1,i},s_{2,i},s_{3,i},\hat{s}_{1,i},\hat{s}_{2,i},\hat{s}_{3,i}\}_{i=1,2,\ldots,T}$
S1108
认证装置的随机数生成部从 0 至 q-1 的
整数中均匀随机地取出 4 次值，设为 $\{u_2,u_3,\hat{u}_2,\hat{u}_3\}$
S1109
认证装置的加密类似度生成部计算
$d_i=(c_i-c'_i)+s_{1,i}w_1+s_{2,i}w_2+s_{3,i}w_3$
S1110
认证装置的加密类似度生成部计算
$\hat{d}_i=(\hat{c}_i-\hat{c}'_i)+\hat{s}_{1,i}\hat{w}_1+\hat{s}_{2,i}\hat{w}_2+\hat{s}_{3,i}\hat{w}_3$
S1111
认证装置的加密类似度生成部计算
$E=\sum_{i=1}^{T}(\hat{s}_{1,i}(c_i-c'_i)+s_{1,i}\hat{s}_{1,i}w_1)+u_2w_2+u_3w_3$
S1112
认证装置的加密类似度生成部计算
$\hat{E}=\sum_{i=1}^{T}s_{1,i}(\hat{c}_i-\hat{c}'_i)+\hat{u}_2\hat{w}_2+\hat{u}_3\hat{w}_3$
S1113
认证装置的通信部将 $(d_1,\ldots,d_T,\hat{d}_1,\ldots\hat{d}_T,E,\hat{E})$
发送到解密装置
S1114
向步骤 S715

图12

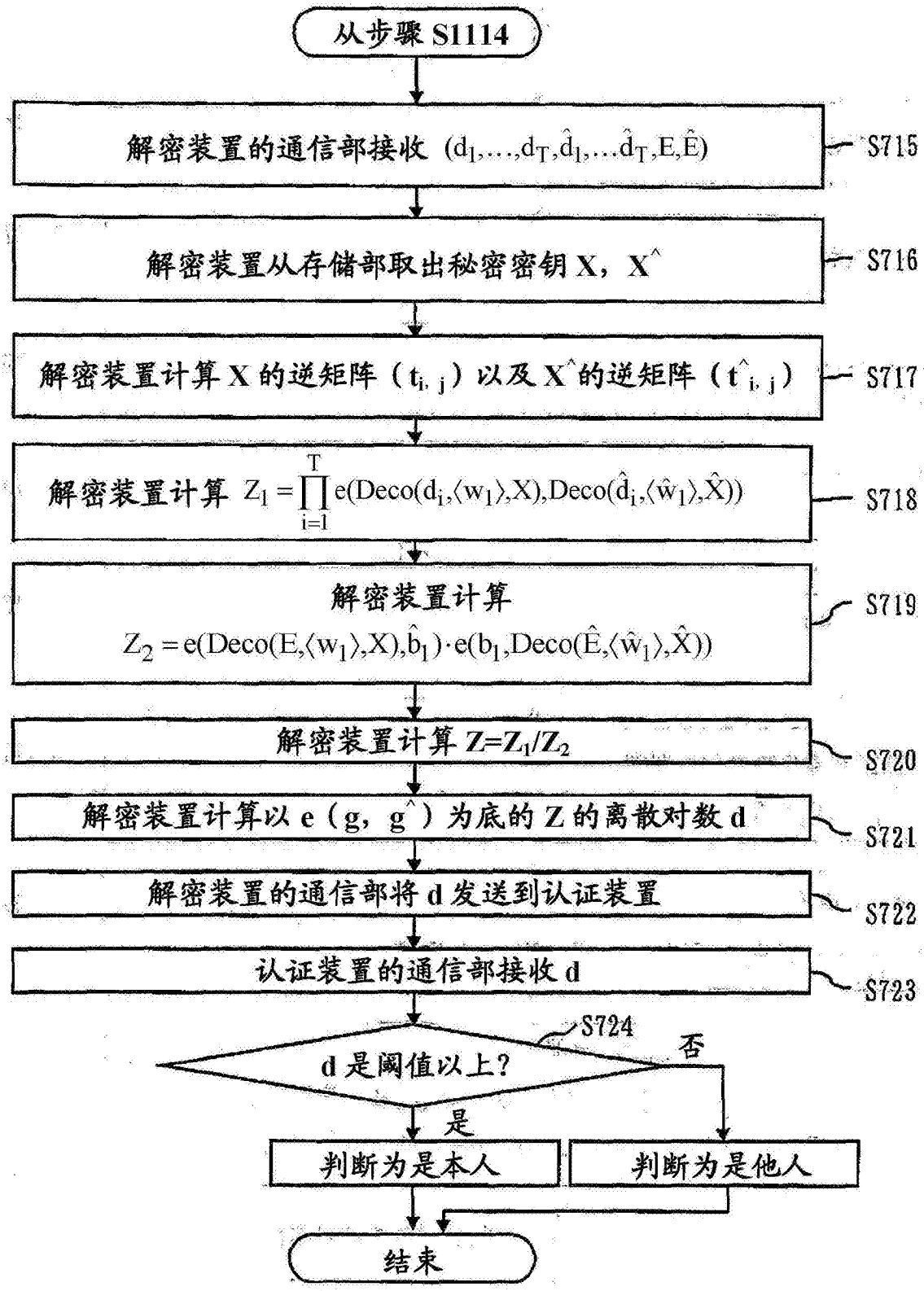

从步骤 S1114
解密装置的通信部接收 $(d_1,\ldots,d_T,\hat{d}_1,\ldots\hat{d}_T,E,\hat{E})$
S715
解密装置从存储部取出秘密密钥 X，X^
S716
解密装置计算 X 的逆矩阵（$t_{i,j}$）以及 X^的逆矩阵（$\hat{t}_{i,j}$）
S717
解密装置计算 $Z_1=\prod_{i=1}^{T} e(Deco(d_i,\langle w_1\rangle,X),Deco(\hat{d}_i,\langle\hat{w}_1\rangle,\hat{X}))$
S718
解密装置计算
$Z_2=e(Deco(E,\langle w_1\rangle,X),\hat{b}_1)\cdot e(b_1,Deco(\hat{E},\langle\hat{w}_1\rangle,\hat{X}))$
S719
解密装置计算 $Z=Z_1/Z_2$
S720
解密装置计算以 e（g，g^）为底的 Z 的离散对数 d
S721
解密装置的通信部将 d 发送到认证装置
S722
认证装置的通信部接收 d
S723
S724
d 是阈值以上？
否
是
判断为是本人
判断为是他人
结束

图13

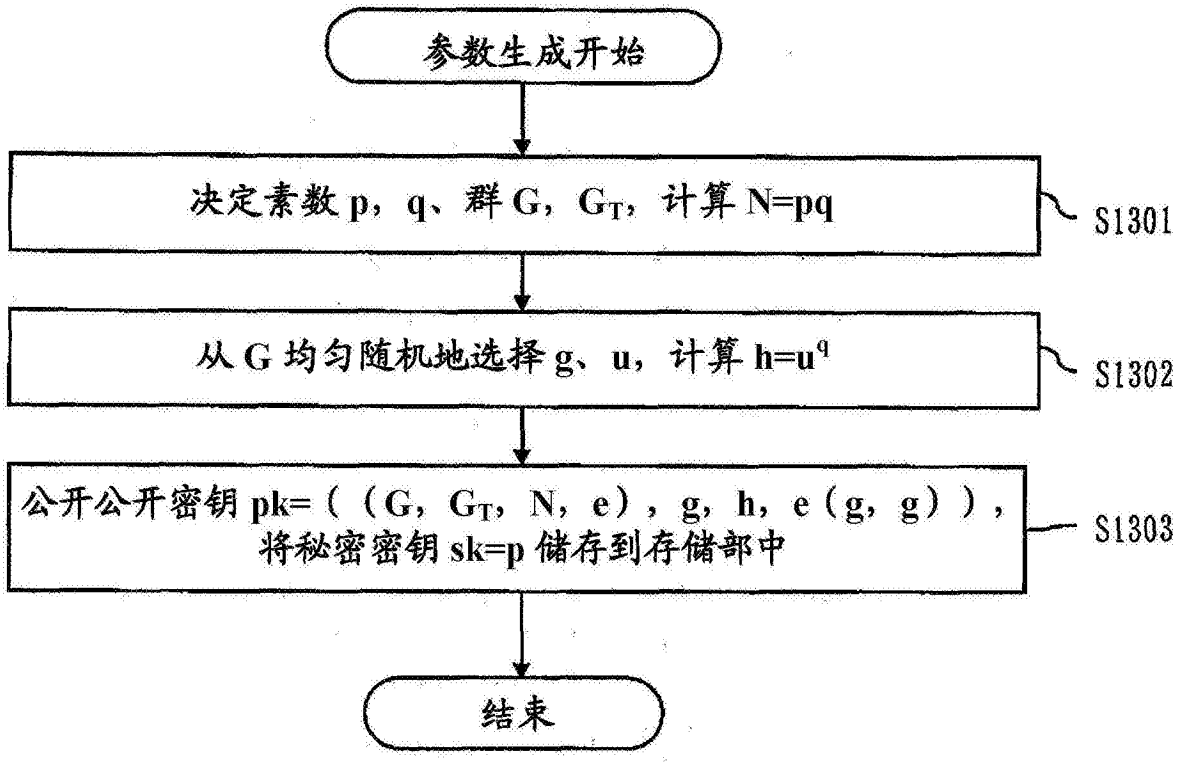

参数生成开始
决定素数 p，q、群 G，G_T，计算 N=pq
S1301
从 G 均匀随机地选择 g、u，计算 $h=u^q$
S1302
公开公开密钥 pk=（（G，G_T，N，e），g，h，e（g，g）），
将秘密密钥 sk=p 储存到存储部中
S1303
结束

图14

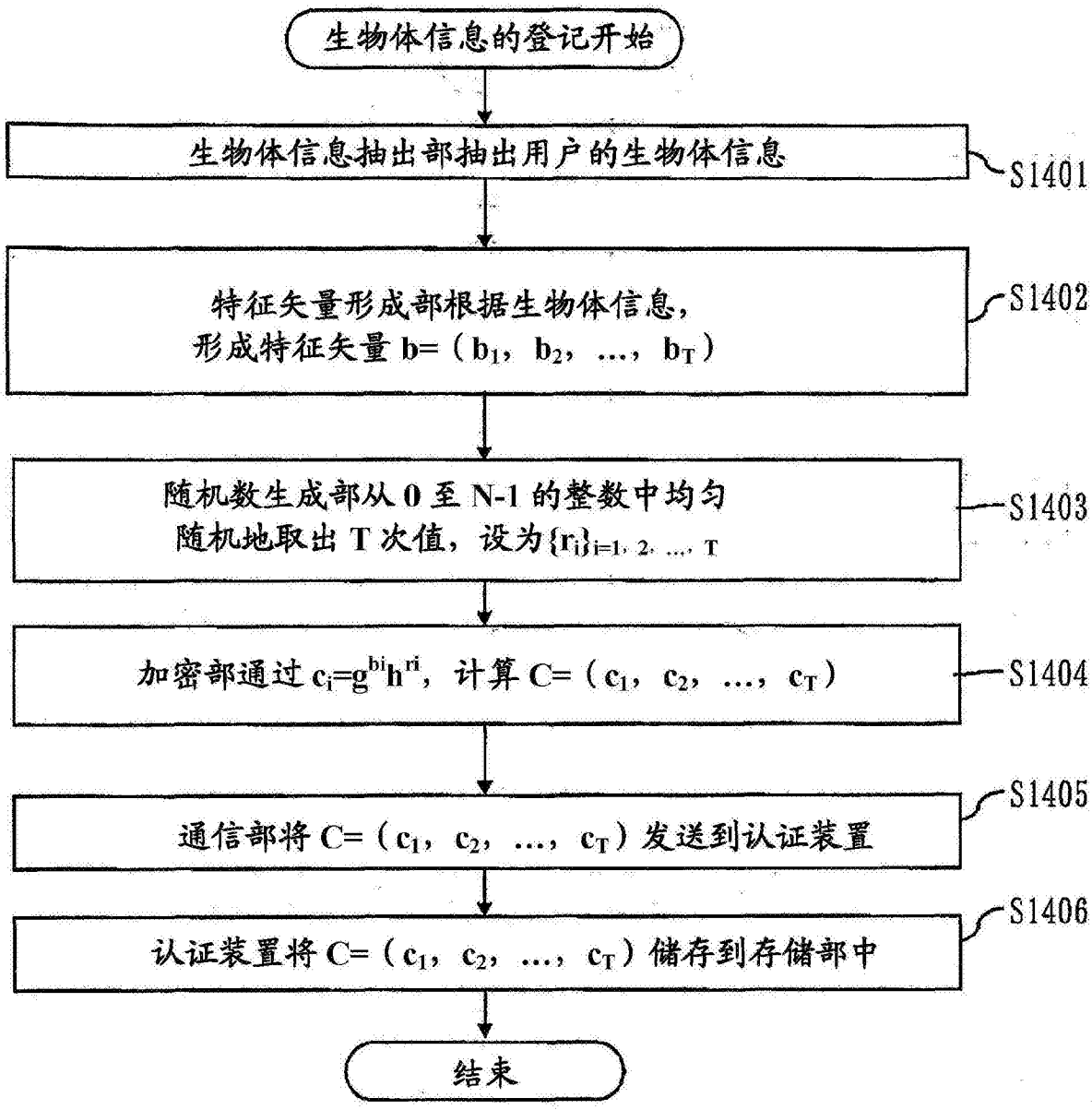

生物体信息的登记开始
生物体信息抽出部抽出用户的生物体信息
S1401
特征矢量形成部根据生物体信息，
形成特征矢量 b=（b_1，b_2，…，b_T）
S1402
随机数生成部从 0 至 N-1 的整数中均匀
随机地取出 T 次值，设为$\{r_i\}_{i=1, 2, \ldots, T}$
S1403
加密部通过 $c_i=g^{bi}h^{ri}$，计算 C=（c_1，c_2，…，c_T）
S1404
通信部将 C=（c_1，c_2，…，c_T）发送到认证装置
S1405
认证装置将 C=（c_1，c_2，…，c_T）储存到存储部中
S1406
结束

图15

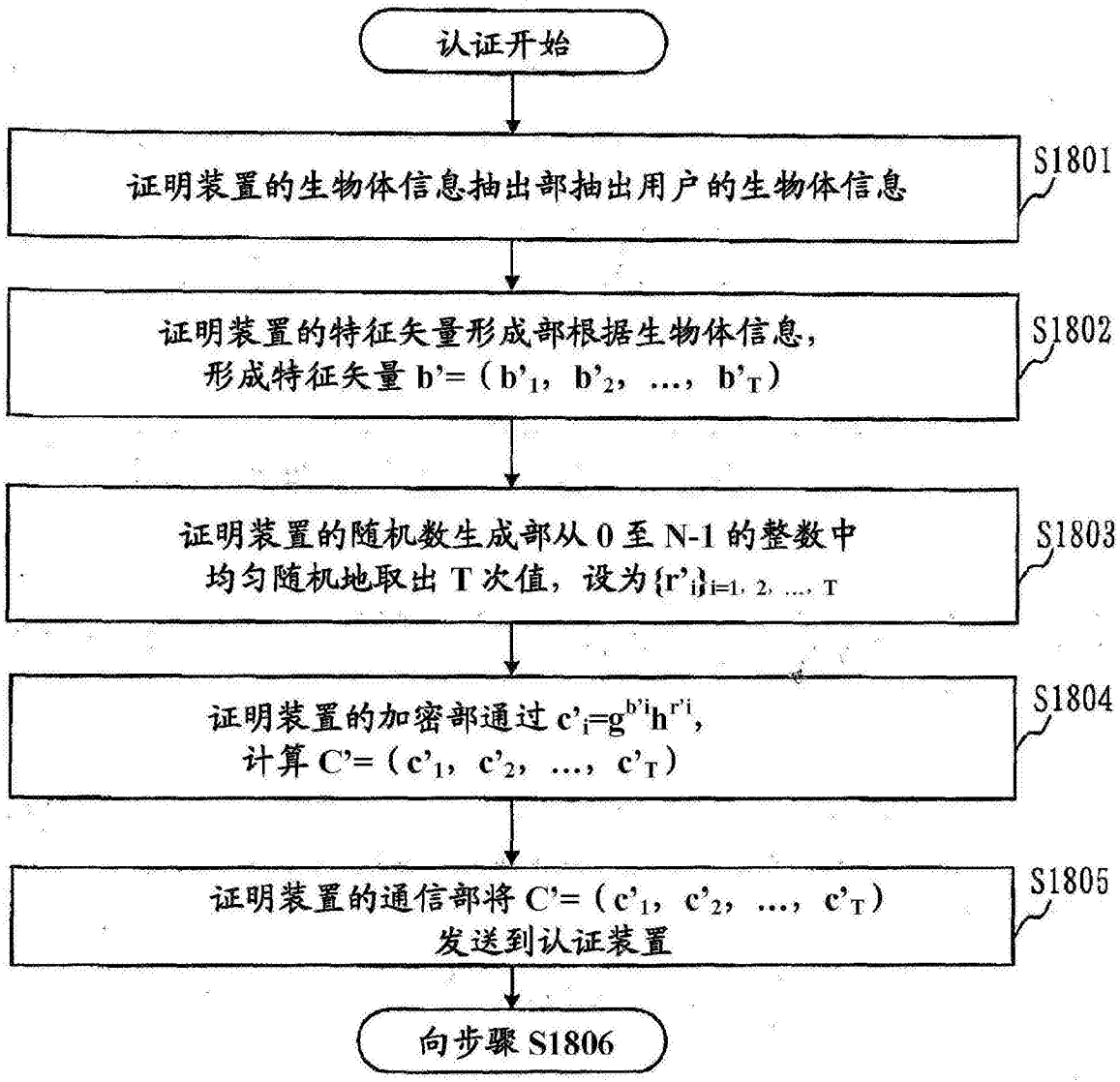

认证开始
证明装置的生物体信息抽出部抽出用户的生物体信息
S1801
证明装置的特征矢量形成部根据生物体信息，
形成特征矢量 b'=（b'1，b'2，…，b'T）
S1802
证明装置的随机数生成部从 0 至 N-1 的整数中
均匀随机地取出 T 次值，设为{r'i}i=1, 2, …, T
S1803
证明装置的加密部通过 c'i=g^b'i h^r'i，
计算 C'=（c'1，c'2，…，c'T）
S1804
证明装置的通信部将 C'=（c'1，c'2，…，c'T）
发送到认证装置
S1805
向步骤 S1806

图16

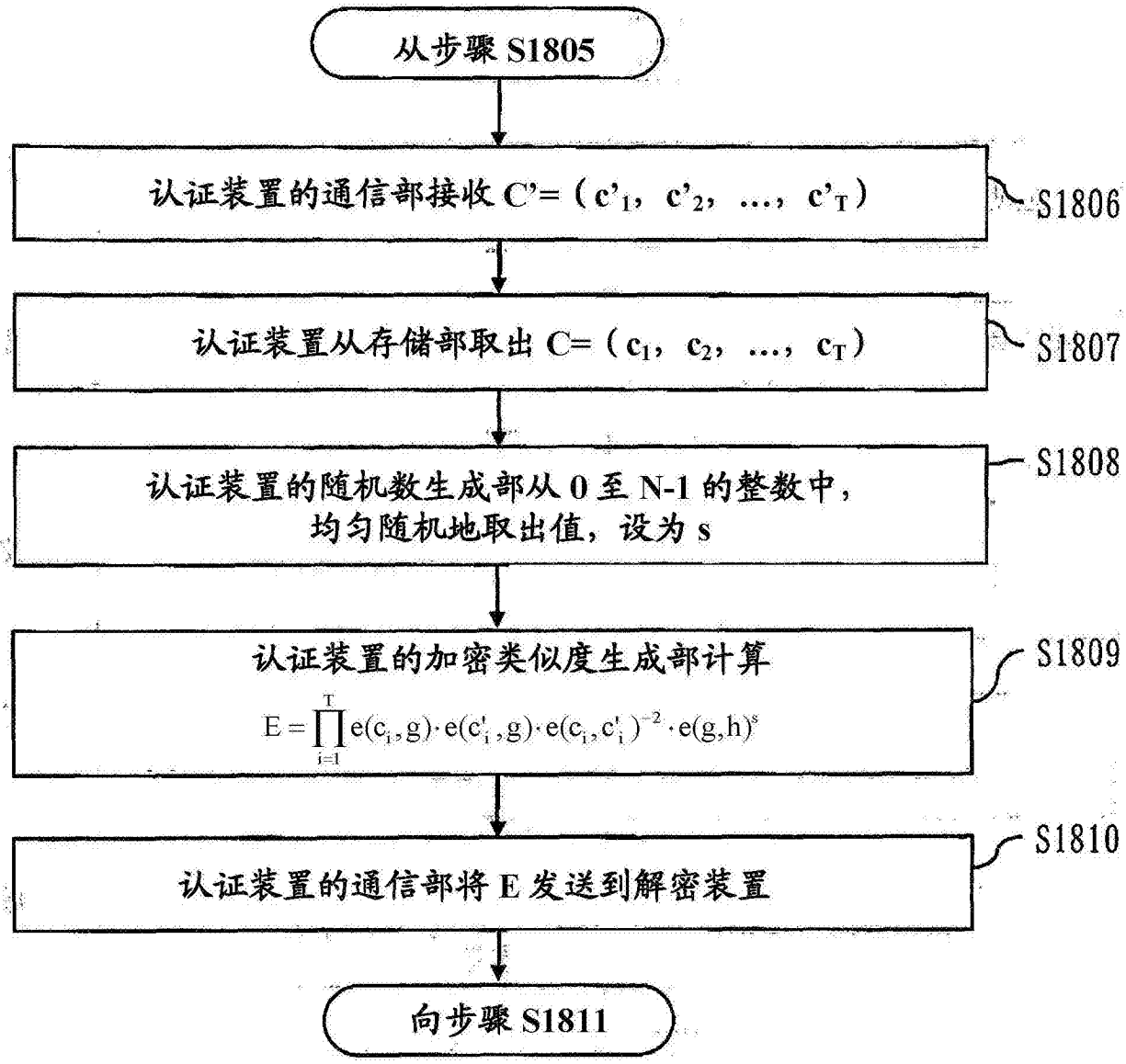

从步骤 S1805
认证装置的通信部接收 C'=（c'1，c'2，…，c'T）
S1806
认证装置从存储部取出 C=（c1，c2，…，cT）
S1807
认证装置的随机数生成部从 0 至 N-1 的整数中，
均匀随机地取出值，设为 s
S1808
认证装置的加密类似度生成部计算
$E=\prod_{i=1}^{T} e(c_i,g)\cdot e(c'_i,g)\cdot e(c_i,c'_i)^{-2}\cdot e(g,h)^{s}$
S1809
认证装置的通信部将 E 发送到解密装置
S1810
向步骤 S1811

图17

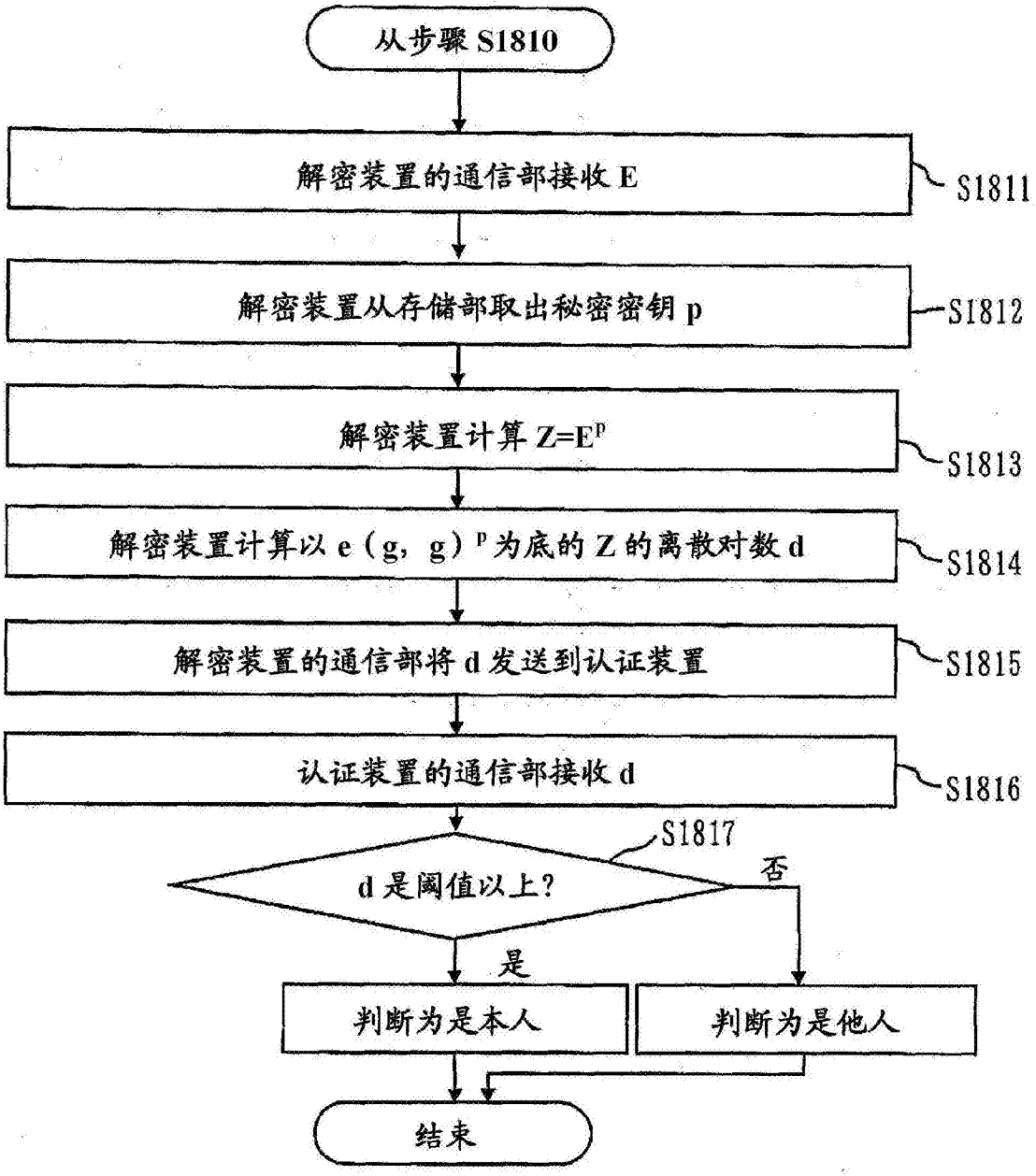

从步骤 S1810
解密装置的通信部接收 E
S1811
解密装置从存储部取出秘密密钥 p
S1812
解密装置计算 Z=E^p
S1813
解密装置计算以 e（g，g）^p 为底的 Z 的离散对数 d
S1814
解密装置的通信部将 d 发送到认证装置
S1815
认证装置的通信部接收 d
S1816
S1817
d 是阈值以上？
否
是
判断为是本人
判断为是他人
结束

图18

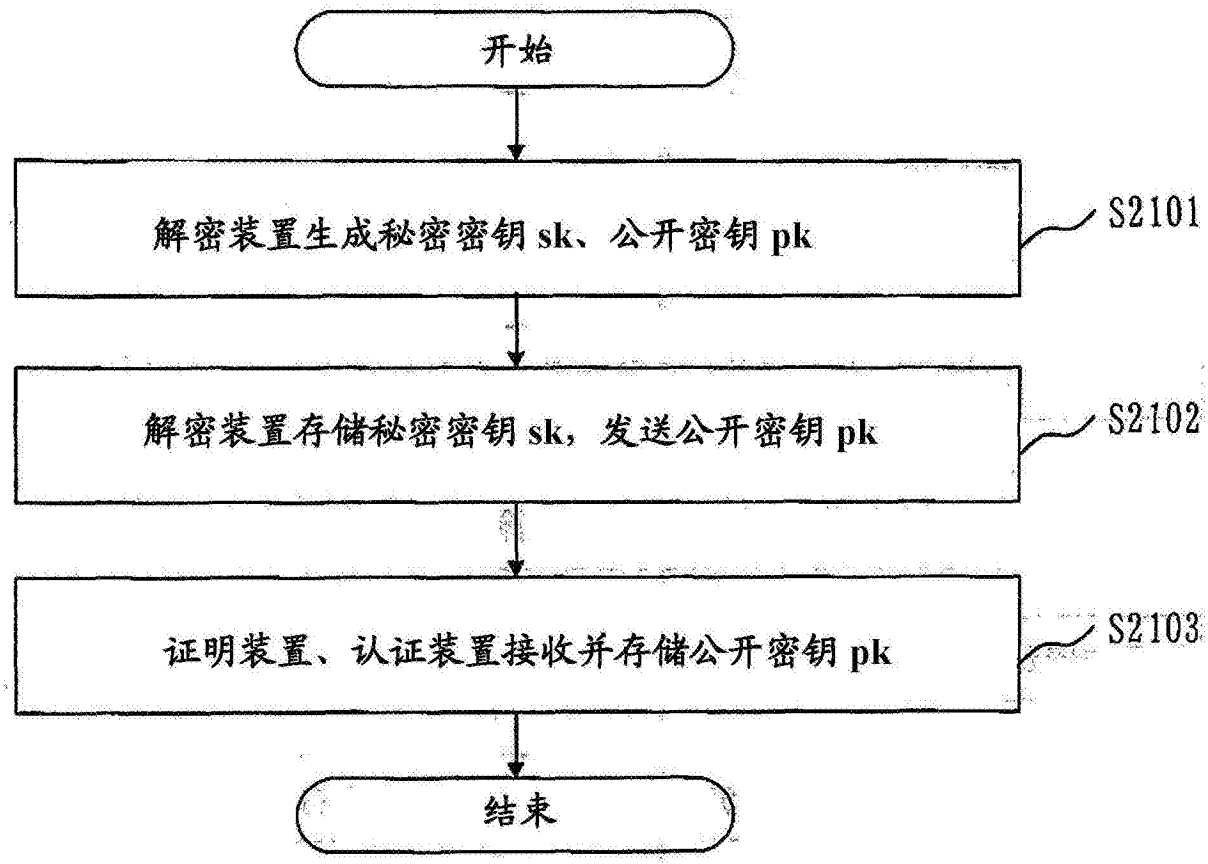

开始
解密装置生成秘密密钥 sk、公开密钥 pk
S2101
解密装置存储秘密密钥 sk，发送公开密钥 pk
S2102
证明装置、认证装置接收并存储公开密钥 pk
S2103
结束

图19

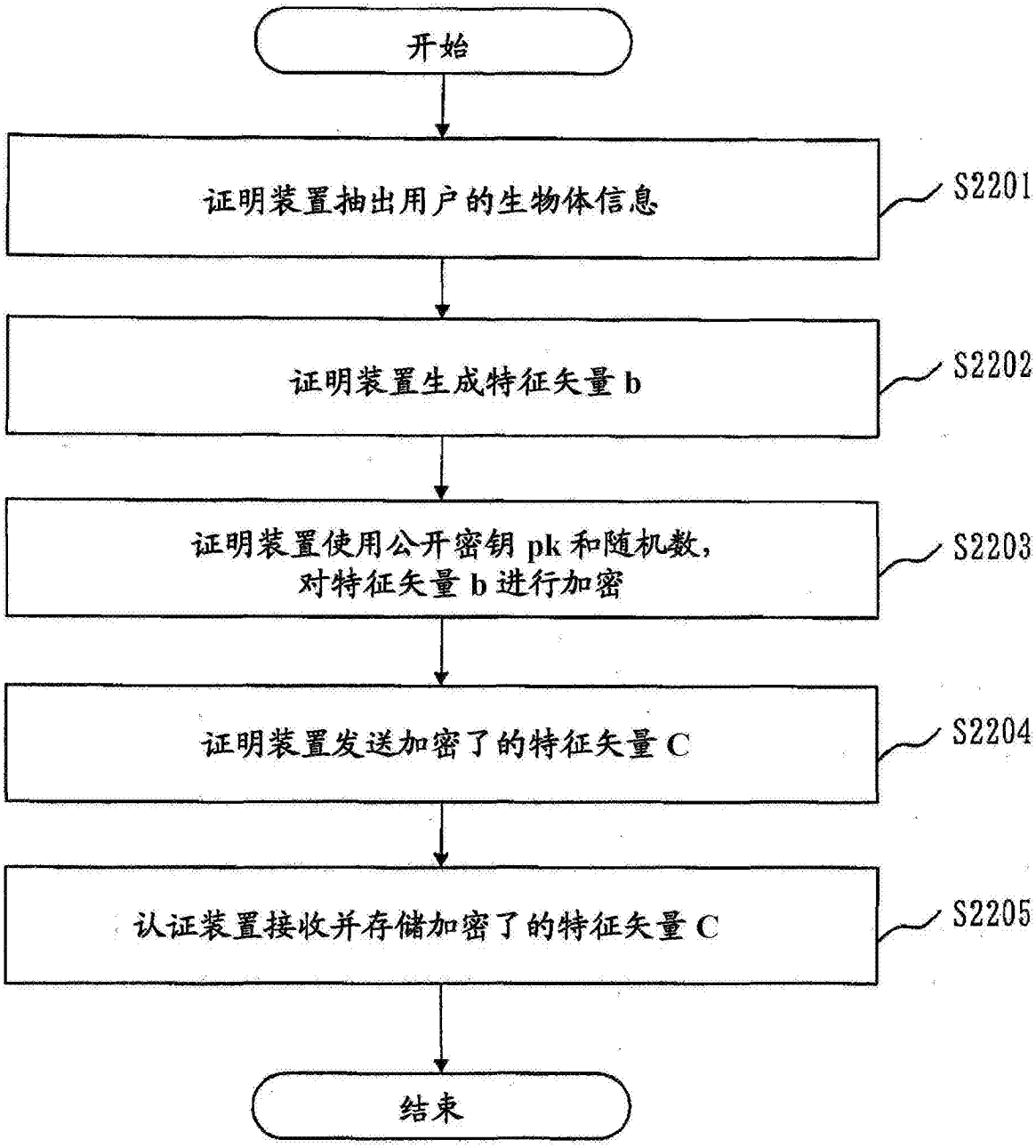

开始
证明装置抽出用户的生物体信息
S2201
证明装置生成特征矢量 b
S2202
证明装置使用公开密钥 pk 和随机数，
对特征矢量 b 进行加密
S2203
证明装置发送加密了的特征矢量 C
S2204
认证装置接收并存储加密了的特征矢量 C
S2205
结束

图20

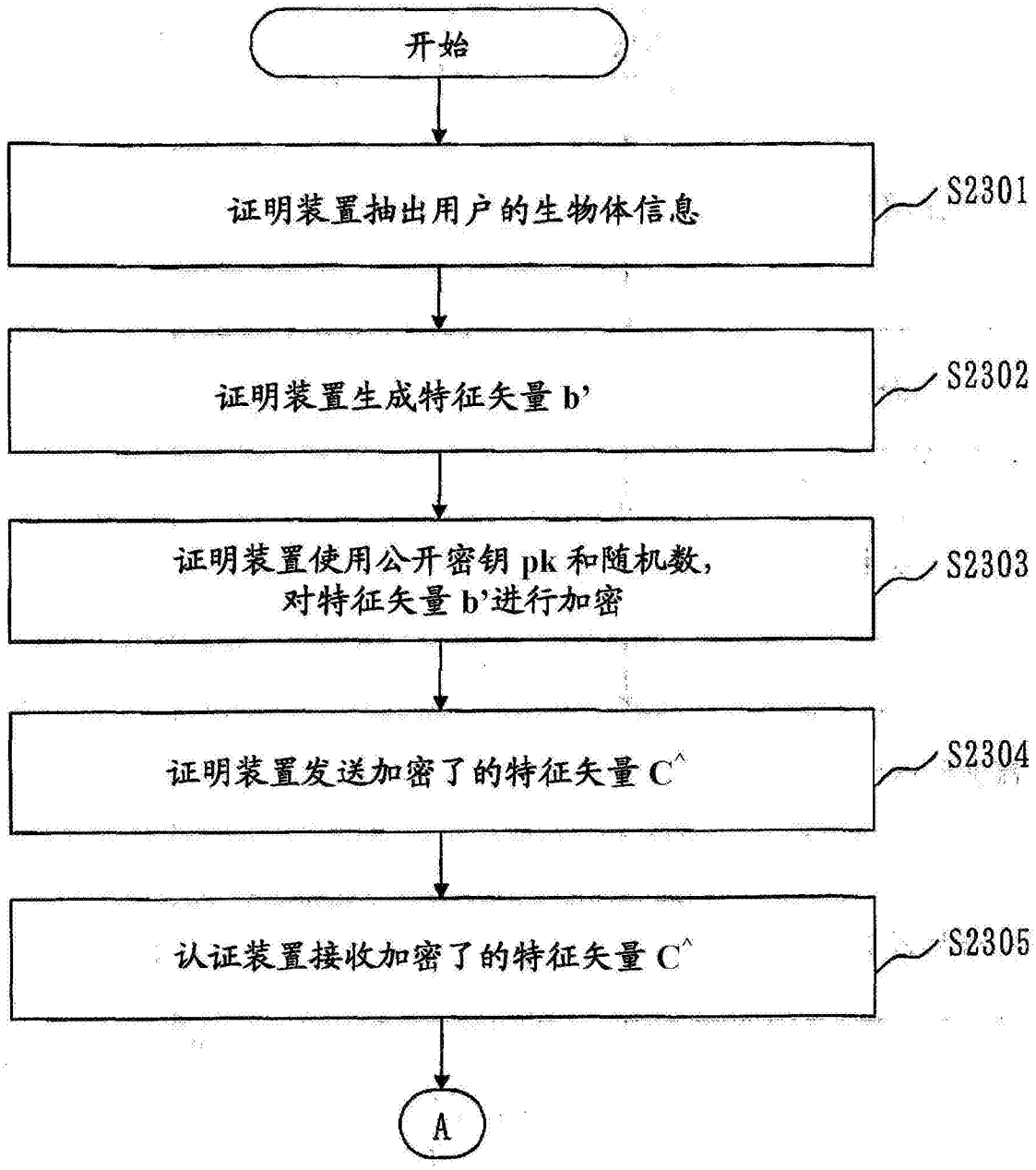

开始
证明装置抽出用户的生物体信息
S2301
证明装置生成特征矢量 b'
S2302
证明装置使用公开密钥 pk 和随机数，
对特征矢量 b'进行加密
S2303
证明装置发送加密了的特征矢量 C^
S2304
认证装置接收加密了的特征矢量 C^
S2305
A

图21

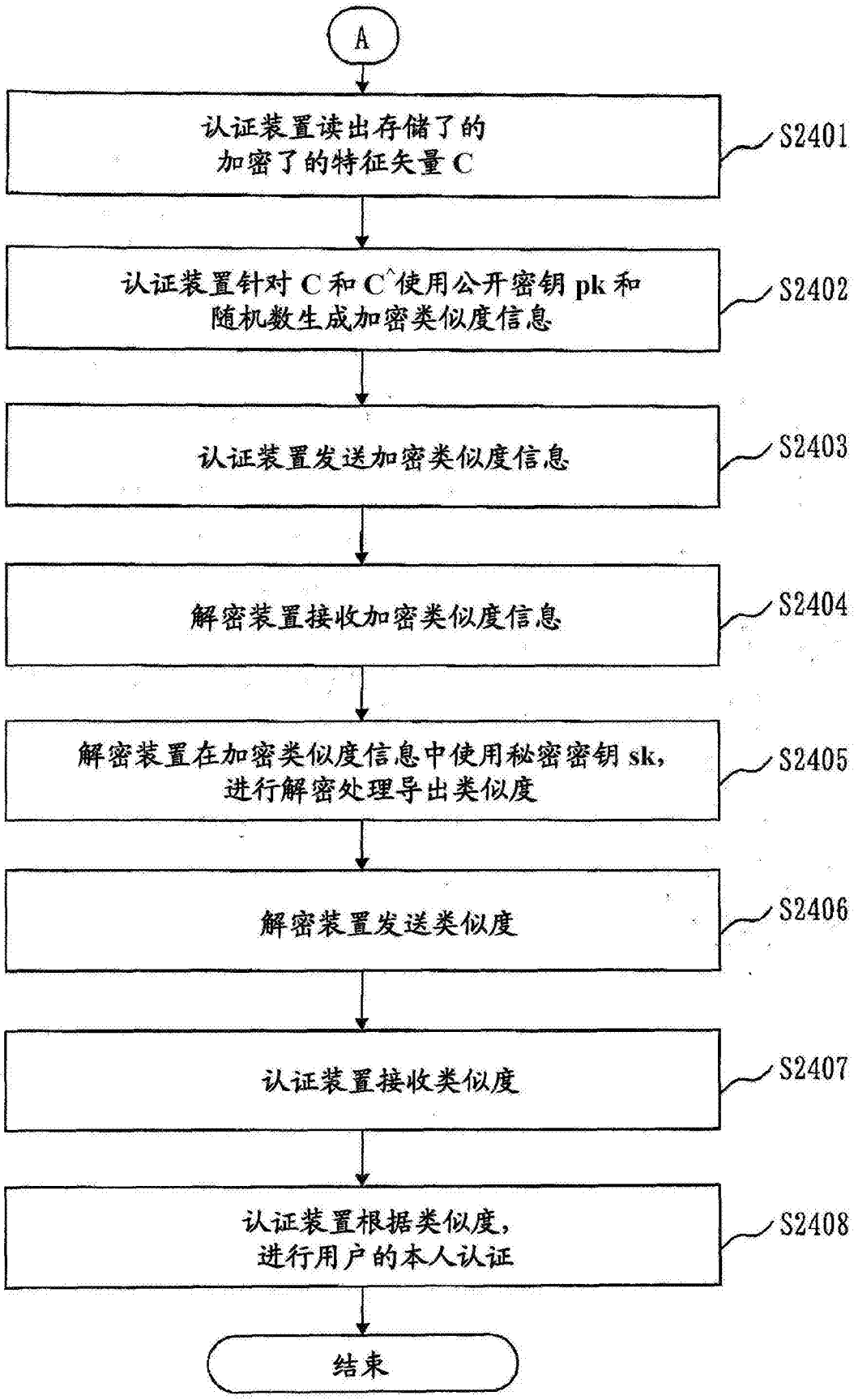

A
认证装置读出存储了的
加密了的特征矢量 C
S2401
认证装置针对 C 和 C^使用公开密钥 pk 和
随机数生成加密类似度信息
S2402
认证装置发送加密类似度信息
S2403
解密装置接收加密类似度信息
S2404
解密装置在加密类似度信息中使用秘密密钥 sk，
进行解密处理导出类似度
S2405
解密装置发送类似度
S2406
认证装置接收类似度
S2407
认证装置根据类似度，
进行用户的本人认证
S2408
结束

图22

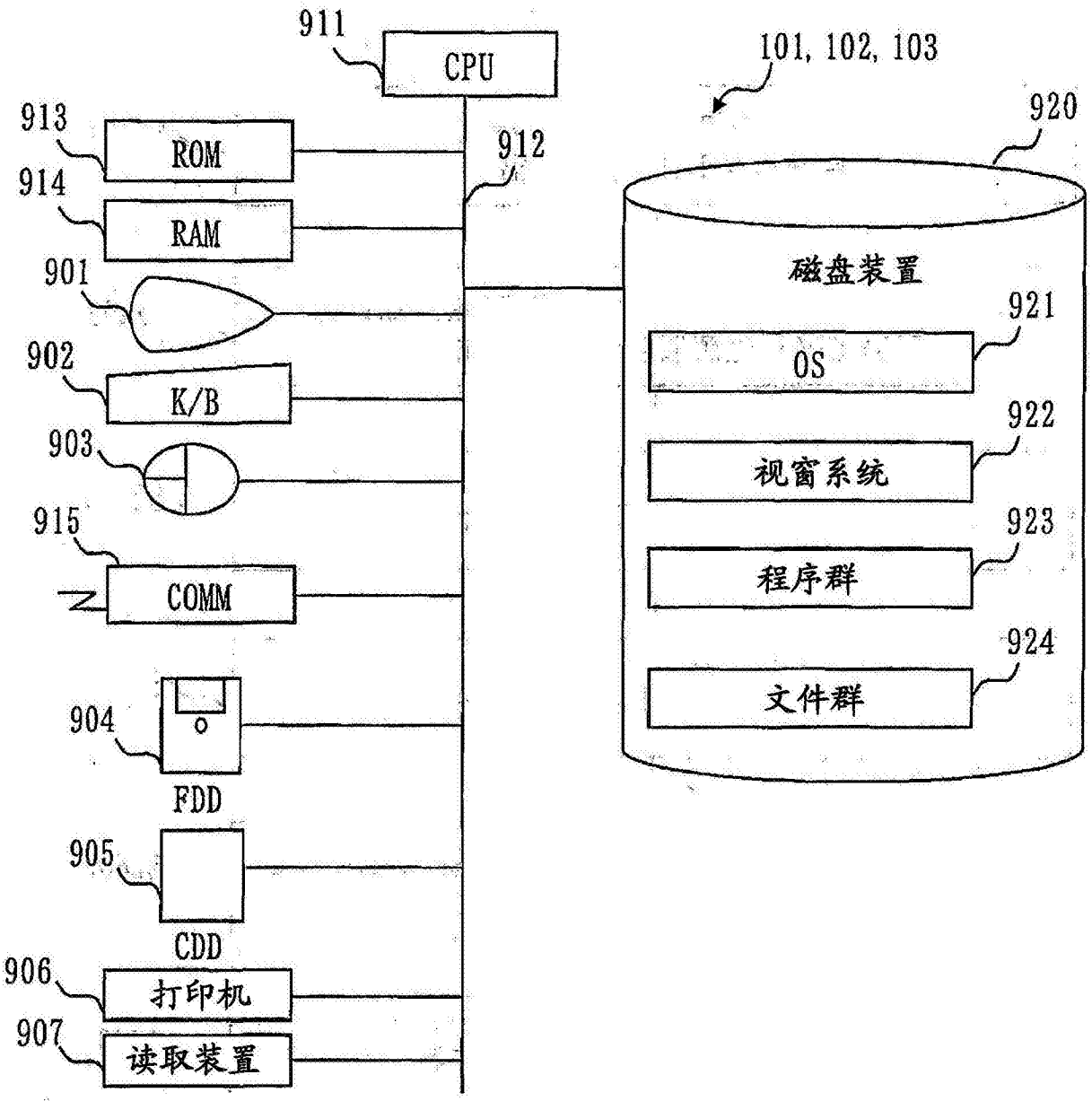

911
CPU
101, 102, 103
920
913
ROM
912
914
RAM
磁盘装置
901
921
OS
902
K/B
922
视窗系统
903
923
程序群
915
COMM
924
文件群
904
FDD
905
CDD
906
打印机
907
读取装置

图23