(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112805704 A
(43)申请公布日 2021.05.14

(21)申请号 201980065945.2
(22)申请日 2019.08.07
(30)优先权数据
2018902873 2018.08.07 AU
(85)PCT国际申请进入国家阶段日
2021.04.06
(86)PCT国际申请的申请数据
PCT/AU2019/050828 2019.08.07
(87)PCT国际申请的公布数据
WO2020/028950 EN 2020.02.13
(71)申请人 黑文技术私人有限公司
地址 澳大利亚悉尼
(72)发明人 韦尔农·默多克 纳文·内蒂 约翰·凯莱塔
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 孙尚白
(51)Int.Cl.
G06F 21/60(2006.01)

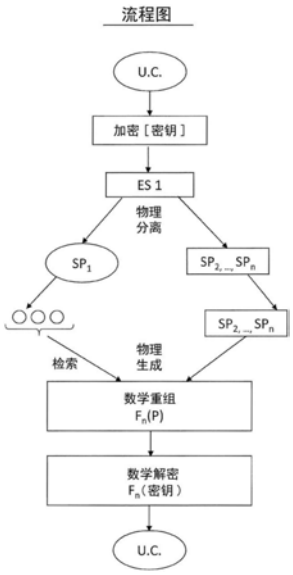
权利要求书6页 说明书14页 附图10页

(54)发明名称

保护数据的方法和系统

(57)摘要

一种加密并存储数据项的方法，所述方法包括：数据加密步骤，其中将数据项加密以形成加密数据项；数学分解步骤，其中将加密数据项在数学上分解为包括至少一个第一分量部分和至少一个第二分量部分在内的两个或更多个加密数据项分量部分；将分量部分中的至少一个分量部分存储在与分量部分中的其他分量部分分离的位置。



CN 112805704 A

1.一种加密并存储数据项的方法,所述方法包括:

a.数据加密步骤,其中将所述数据项加密以形成加密数据项;

b.数学分解步骤,其中将所述加密数据项在数学上分解为包括至少一个第一分量部分和至少一个第二分量部分在内的两个或更多个加密数据项分量部分;

c.将所述分量部分中的至少一个分量部分存储在与所述分量部分中的其他分量部分分离的位置。

2.根据权利要求1所述的方法,其中,位置分离是通过逻辑存储器分离进行的,由此所述至少一个第一分量部分被存储在第一逻辑存储器中,并且所述至少一个第二分量部分被存储在第二逻辑存储器中。

3.根据权利要求1所述的方法,其中,位置分离是通过使用分离的服务器进行的,由此所述至少一个第一分量部分被存储在第一服务器中,并且所述至少一个第二分量部分被存储在第二服务器中。

4.根据权利要求1所述的方法,其中,位置分离是通过地理分离进行的,由此所述至少一个第一分量部分被存储在第一地理位置,并且所述至少一个第二分量部分被存储在第二地理位置,并且其中所述第一地理位置与所述第二地理位置在地理上分离。

5.根据权利要求4所述的方法,其中,所述位置分离是分离的服务器的地理分离,每个服务器保持形成所述加密数据项的所述分量部分中的不同分量部分。

6.根据权利要求1所述的方法,其中,所述数据加密步骤包括以下步骤:在对所述数据项进行加密的算法中,使用加密密钥作为参数来对所述数据项进行加密。

7.根据权利要求1所述的方法,其中,在所述数据加密步骤之前填充所述数据项。

8.根据权利要求7所述的方法,其中,所述加密密钥是对称密钥。

9.根据权利要求7所述的方法,其中,在所述数学分解步骤之前,通过加密数据项映射步骤对所述加密数据项进行映射,以形成经映射的加密数据项。

10.根据权利要求1至9中的任一项所述的方法,其中,所述数学分解步骤包括在将所述加密数据项拆分成分量部分的算法中使用分解密钥作为参数。

11.根据权利要求10所述的方法,其中,所述分解密钥是质数。

12.根据权利要求10所述的方法,其中,所述分解密钥是对称密钥。

13.根据权利要求1至12中的任一项所述的方法,其中,所述数据项是参考凭证来存储的。

14.根据权利要求1至12中的任一项所述的方法,其中,所述数据项与实体相关联。

15.根据权利要求13所述的方法,其中,所述凭证是所述数据项与实体相关联的所述实体的实体凭证。

16.根据任一前述权利要求所述的方法,其中,在特定形式中,所述算法是不可反转的,使得仅拥有所述算法的变量中的其他变量中的不管哪一个变量是无法获得输入到所述算法17中的数据项字符串16的。

17.一种保护数据项N以用于安全存储所述数据项的表示的方法,所述数据项具有数据项字符串的形式,所述方法包括以下步骤:

a.将包括所述数据项在内的字符串导入第一环境;

b.将具有至少一个第一数据项变量的第一算法应用于所述数据项字符串,从而形成第

一修改数据项字符串；

c.将具有至少一个第二数据项变量的第二算法应用于所述第一修改字符串，由此将所述第一修改数据项字符串嵌入第二修改数据项字符串中，所述第二修改数据项字符串具有第一数据项质数的形式；

d.选择与所述第一数据项质数不同的第二数据项质数；

e.至少将所述第一数据项质数定义为关于所述数据项的数据项私钥；将所述第一数据项质数和所述第二数据项质数的乘积定义为关于所述数据项的数据项公钥；

f.从所述第一环境中删除所述数据项字符串；

g.维持与所述第一数据项质数、所述第一算法和所述第二算法相关联的数据记录，从而能够通过向所述第一算法和所述第二算法提供变量来计算所述数据项。

18.根据权利要求17所述的方法，其中，变量是所述数据项公钥。

19.根据权利要求17所述的方法，其中，变量是所述数据项私钥。

20.根据权利要求17所述的方法，其中，变量是所述第二数据项变量。

21.根据权利要求17所述的方法，其中，变量是所述第一数据项变量。

22.根据权利要求20所述的方法，其中，所述第二数据项变量是数值增量。

23.根据权利要求21所述的方法，其中，所述第一数据项变量是ASCII查找表。

24.根据权利要求17至23中的任一项所述的方法，其中，所述第一算法将所述字符串转换为数字串。

25.根据权利要求17至24中的任一项所述的方法，其中，所述第二算法将数值增量添加到所述第一修改字符串，以形成所述第二修改字符串。

26.根据前述权利要求17至25中的任一项所述的方法，其中，在特定形式中，所述算法是不可反转的，使得仅拥有所述算法的变量中的其他变量中的不管哪一个变量是无法获得输入到所述算法17中的数据项字符串16的。

27.一种保护数据项N以用于安全地存储所述数据项的至少两个表示和至少两个数据项变量的方法，所述数据项N以数据项字符串的形式表示，所述数据项变量包括用于至少两种算法的变量，所述至少两种算法接收所述数据项的表示作为输入并输出所述数据项的表示的修改形式，所述方法包括以下步骤：

a.将所述数据项字符串导入第一环境；

b.将具有至少一个第一数据项变量的第一算法应用于所述数据项字符串，从而形成第一修改数据项字符串；

c.将具有至少一个第二数据项变量的第二算法应用于所述第一修改字符串，从而形成第二修改数据项字符串；

d.从所述第一环境中删除所述数据项字符串；

e.将所述第一修改数据项字符串、所述第二修改数据项字符串、所述第一数据项变量和所述第二数据项变量中的一个或多个移动到第二环境；

f.所述第二环境位于与所述第一环境相距较远的位置。

28.根据权利要求27所述的方法，其中，维持所述数据项字符串、所述第一算法和所述第二算法的记录，从而能够通过向所述第一算法和所述第二算法提供变量来计算所述数据项。

29.根据权利要求27所述的方法,其中,变量是所述数据项公钥。

30.根据权利要求27所述的方法,其中,变量是所述数据项私钥。

31.根据权利要求27所述的方法,其中,变量是所述第二数据项变量。

32.根据权利要求27所述的方法,其中,变量是所述第一数据项变量。

33.根据权利要求27所述的方法,其中,所述第二数据项变量是数值增量。

34.根据权利要求27所述的方法,其中,所述第一数据项变量是ASCII查找表。

35.根据权利要求27所述的方法,其中,所述第一函数将所述字符串转换为数字串。

36.根据权利要求27所述的方法,其中,所述第二算法将数值增量添加到所述第一修改字符串,以形成所述第二修改字符串,由此将所述第一修改数据项字符串嵌入第二修改数据项字符串中,所述第二修改数据项字符串具有第一数据项质数的形式;选择与所述第一数据项质数不同的第二数据项质数;至少将所述第一数据项质数定义为关于所述数据项的数据项私钥;将所述第一数据项质数和所述第二数据项质数的乘积定义为关于所述数据项的数据项公钥。

37.根据权利要求27所述的方法,其中,变量紧邻在其应用到算法之前被动态创建。

38.根据权利要求27或权利要求28所述的方法,其中,每个辅助变量紧邻在其应用到算法之前被动态创建。

39.根据权利要求27所述的方法,其中,辅助变量中的至少一些辅助变量紧邻在其作为算法的输入而应用之前被动态创建。

40.根据权利要求27所述的方法,其中,所述算法被应用于第一环境20内的所述数据项字符串。

41.根据权利要求40所述的方法,其中,一旦已经应用了所述算法,就将所述变量中的一个或多个变量存储在第二环境21中。

42.根据权利要求27所述的方法,其中,主要变量中的至少一个主要变量被存储在所述第二环境中,优选地,所述主要变量中的至少一个主要变量被存储在所述第二环境中,然后所述至少一个主要变量从所述第一环境中被删除。

43.根据权利要求27所述的方法,其中,辅助变量中的至少一个辅助变量被存储在所述第二环境中,在优选的形式中,所述辅助变量中的至少一个辅助变量被存储在所述第二环境中,然后所述至少一个辅助变量从所述第一环境中被删除。

44.根据权利要求27所述的方法,其中,至少一个第一算法14和至少一个第二算法17连续地应用于所述数据项字符串13,在优选形式中,在将所述至少一个第一算法14和所述至少一个第二算法17应用于所述数据项字符串13之后,至少一个主要变量和至少一个辅助变量被存储在所述第二环境中。

45.根据权利要求27至44中的任一项所述的方法,其中,所述过程被重复N次。

46.根据权利要求45所述的方法,其中,N等于2。

47.根据权利要求45所述的方法,其中,N等于3。

48.根据权利要求45所述的方法,其中,N等于4。

49.根据权利要求27至48中的任一项所述的方法,其中,在将至少一个主要变量和所述至少一个辅助变量存储在所述第二环境中之后,所述至少一个主要变量和所述至少一个辅助变量从所述第一环境中被删除。

50.根据权利要求27至49中的任一项所述的方法，其中，所述第二环境21与所述第一环境20分离。

51.根据权利要求50所述的方法，其中，通过使所述第二环境位于与所述第一环境的位置相距较远的位置，所述第二环境21与所述第一环境20分离。

52.根据权利要求50所述的方法，其中，所述第二环境21与所述第一环境20在逻辑上分离。

53.根据权利要求27至52中的任一项所述的方法，其中，存储在所述第二环境中的那些输出或变量然后从所述第一环境中被删除。

54.根据权利要求27至53中的任一项所述的方法，其中，一旦已经应用了所述算法中的一种或多种算法，包括所述数据项字符串13在内的所述数据项11就从所述第一环境中被删除。

55.根据权利要求27至54中的任一项所述的方法，其中，一旦已经应用了所述算法中的一种或多种算法并且一旦将所述算法的输出中的一个或多个输出或所述变量中的一个或多个变量存储在所述第二环境21中，包括所述数据项字符串13在内的所述数据项11就从所述第一环境中被删除。

56.根据权利要求27至55中的任一项所述的方法，其中，当期望恢复所述数据项11中包含的信息12时，反转上述过程。

57.根据权利要求56所述的方法，其中，所述反转的第一步是将存储在所述第一环境20和所述第二环境21中的算法的输出或变量置于一个位置。

58.根据权利要求57所述的方法，其中，所述变量然后被应用于所述算法以反转所述过程，由此恢复所述数据项11以供使用。

59.根据权利要求27至58中的任一项所述的方法，其中，在已经使用了所述数据项11之后，将上述过程重新应用于所述数据项11，从而再次保护所述数据项11中包含的所述信息12达潜在的不确定时间段。

60.根据权利要求27至59中的任一项所述的方法，其中，所述算法是不可反转的，使得仅拥有所述算法的变量中的其他变量中的不管哪一个变量是无法获得输入到所述算法17中的所述数据项字符串16的。

61.一种保护数据项N中的信息的方法，所述数据项N以数据项字符串的形式表示，所述方法包括以下步骤：

a.将所述数据项字符串导入第一环境；

b.将具有至少一个第一数据项主要变量和至少一个第一数据项辅助变量的至少一个第一算法应用于所述数据项字符串，从而形成第一修改数据项字符串，并且其中所述至少一个第一数据项主要变量包括所述数据项字符串；

c.将具有至少一个第二数据项主要变量和至少一个第二数据项辅助变量的第二算法应用于所述第一修改字符串，从而形成第二修改数据项字符串，并且其中所述至少一个第二数据项主要变量包括所述第一修改数据项字符串；

d.从所述第一环境中删除所述数据项字符串；

e.将所述变量中的一个或多个变量移动到至少一个第二环境；

f.所述第二环境位于与所述第一环境相距较远的位置。

62.根据权利要求61所述的方法，用于安全存储所述数据项的至少两个表示和至少两个数据项变量，所述数据项变量包括用于至少两种算法的变量，所述至少两种算法接收所述数据项的表示作为输入，并输出所述数据项的表示的修改形式。

63.根据权利要求61或62所述的方法，其中，变量包括所述第一修改数据项字符串、所述第二修改数据项字符串、所述第一数据项变量和所述第二数据项变量中的一个或多个。

64.根据权利要求61至63中的任一项所述的方法，其中，所述算法是不可反转的，使得仅拥有所述算法的变量中的其他变量中的不管哪一个变量是无法获得输入到所述算法17中的所述数据项字符串16的。

65.一种数字输入/输出设备，包括用于实现根据权利要求1至64中的任一项所述的方法的装置。

66.根据权利要求65所述的设备，所述设备被实现为智能电话上的软件应用。

67.一种存储有代码的介质，当由处理器执行所述代码时，所述代码实现根据权利要求1至64中的任一项所述的方法。

68.根据权利要求67所述的介质，其中，所述介质是非暂时性介质。

69.一种数字输入/输出设备，包括用于基于根据权利要求1至64中的任一项所述的方法来识别准备传输数据项的物理特征。

70.根据权利要求69所述的设备，所述设备被实现为智能电话上的软件应用。

71.一种对至少具有第一存储位置和第二存储位置的系统中的安全入侵作出响应的方法，所述系统实现一种加密并存储数据项的方法，所述方法包括：

a.数据加密步骤，其中将所述数据项加密以形成加密数据项；

b.数学分解步骤，其中将所述加密数据项在数学上分解为包括至少一个第一分量部分和至少一个第二分量部分在内的两个或更多个加密数据项分量部分；

c.将所述分量部分中的至少一个分量部分存储在所述第一存储位置，并且将所述第二分量部分存储在与所述分量部分中的其他分量部分分离的所述第二存储位置，所述方法包括：

如果在所述第一位置处检测到安全入侵，使得所述至少一个第一分量部分受到损害：

从所述第一位置删除所述至少一个第一分量部分；以及

从所述第二位置删除所述至少一个第二分量部分。

72.一种分布式加密系统，其中，

a.将要加密的数据放置在主服务器上，然后对所述要加密的数据进行扩展和混淆以形成混淆串；

b.然后使用对称加密密钥对所述混淆串进行加密，以形成加密串；

c.然后将打包数据的串逐步添加到所述加密串，直到得到的数据串在计算上等同于最接近的质数，然后将所述最接近的质数定义为初始质数；

d.生成相似长度的附加质数，并且利用预定的公钥算法，使用所述初始质数和所述附加质数来生成公钥。

73.根据权利要求72所述的分布式加密系统，其中，所述初始质数从存储器中被删除并且未被存储。

74.根据权利要求72或73所述的分布式加密系统，其中，所得的分量然后被存储在不同

的位置。

75.根据权利要求74所述的分布式加密系统,其中,所述对称加密密钥和打包数据的串被存储在主服务器上,所述公钥被存储在辅助服务器上,并且所述附加质数被存储在第三服务器上。

76.根据权利要求72至75中的任一项所述的分布式加密系统,其中,当要对数据解密时,

a.从相应的服务器中检索所述公钥和所述附加质数;

b.利用预定公钥算法,将所述公钥与所述附加质数结合使用,以计算所述初始质数;

c.然后从所得的质数中减去所存储的打包数据的串,并使用所述主服务器上存储的所述对称加密密钥对所得的加密串进行解密;以及

d.使用反向的最初用于原始混淆数据的混淆规则,根据所得的扩展混淆数据串对期望目标数据进行去混淆。

77.根据权利要求72至76中的任一项所述的分布式加密系统,其中,所述系统使用任何形式的公钥加密,包括但不限于RSA或Shamir算法。

78.一种数据保护的方法,所述方法包括以下步骤:

a.用对称密钥对要加密的数据进行加密;

b.混淆并扩展所述对称密钥;

c.然后使用第二对称密钥对经混淆并扩展的所述对称密钥进行加密,然后将所述第二对称密钥存储在主服务器上;

d.然后将打包数据的串添加到加密对称密钥以形成质数;

e.生成相似长度的第二质数,并且两个质数。

79.根据权利要求78所述的方法,其中,所述对称加密密钥和打包数据的串被存储在主服务器上,所述公钥被存储在辅助服务器上,并且所述附加质数被存储在第三服务器上。

80.根据权利要求79所述的方法,其中,通过反转所述步骤来执行数据的解密。

保护数据的方法和系统

技术领域

[0001] 本发明涉及一种用于保护数据的方法和系统，并且更具体地但非排他地涉及结合了多种策略的使用的系统。

背景技术

[0002] 诸如数据混淆和加密等的技术是本领域中众所周知的用于保护数据的方法。数据混淆通常涉及使用随机密钥集对数据进行补偿。

[0003] 除了该操作方法之外，还尝试在网络上的各种隐蔽的地方隐藏数据。这种技术通常称为“通过隐蔽性实现安全性”。该技术是众所周知的，并且通常仅在黑客在网络上的时间有限的情况下才有效。在当今的黑客环境中，这不是一种可防御的策略。

[0004] 存在的其他问题是集中存储用于加密系统的密钥以及集中存储已加密和受保护的数据的通常做法。这两种做法都使黑客很容易找到并攻击数据和密钥存储。

[0005] 在又一通常做法中，使用加密密钥来保护多组受保护的数据意味着对一个数据集成功攻击将导致对所有数据集成功攻击。

[0006] Sun Microsystems的US7,685,430利用了加密算法的多种应用。在这种情况下，将这些技术应用于在互联网托管环境中提供临时密码(尤其是一次性密码)的情况。

[0007] 在US7,685,430的布置中，用于加密算法的密钥包括静态数据，也就是说，在加密算法的多个实例中重复使用相同数据。

[0008] 另外，US7,685,430没有描述用于分割数据以将数据的一部分存储在分布式位置中的任何策略。

[0009] 本申请的布置旨在用于有时需要保留相当长的时间段-大约一年或更长时间的数据。它特别适合且适用于具有商业意义的数据-也就是说，往往是黑客团体的特别有吸引力的目标的数据-即所谓的“蜜罐”。这样的数据可以包括信用卡数据、服务器证书等。

[0010] 要注意的是，存储此类数据的人员现在承担着非常严重的责任。在许多管辖区中，如果确定已发生违规行为，则至少有强制性报告要求。

[0011] 当前，还未使用用于受保护的数据和加密密钥的超出与分布式远程存储技术相结合的标准策略的强大混淆系统。

[0012] 所描述的发明旨在解决这些问题。

发明内容

[0013] 定义

[0014] 混淆：通过使用应用于数据或代码的算法来隐藏数据或代码。需要了解算法，才能揭示已隐藏的数据或代码。

[0015] 字母数字元素：从数字或字母或特殊字符中选择的单个字符。

[0016] 字符串：两个或更多个字符连接成单个字符串。

[0017] 数据加密：将算法应用于输入字符串，算法输出与输入字符串不同的字符串。输出

字符串是输入字符串的加密。输入字符串可从输出字符串中恢复，但要使用解密参数或变量(在某些情况下称为密钥)。控制对参数或变量的访问，从而仅授权方可以从输出字符串中恢复(或解密)输入字符串。

[0018] 数据填充：向字符串添加字符，从而延长字符串。

[0019] 数据映射：利用查找表将字符转换为字符串-例如，可以通过使用ASCII转换表将字母数字字符转换为数字串。

[0020] 较远的位置：通过距离或逻辑与另一个位置分离的位置。

[0021] 因此，在本发明的一种广泛形式中，提供了一种加密并存储数据项的方法；所述方法包括：

[0022] • 数据加密步骤，其中将数据项加密以形成加密数据项；

[0023] • 数学分解步骤，其中将加密数据项在数学上分解为包括至少一个第一分量部分和至少一个第二分量部分在内的两个或更多个加密数据项分量部分；

[0024] • 将分量部分中的至少一个分量部分存储在与分量部分中的其他分量部分分离的位置。

[0025] 优选地，位置分离是通过逻辑存储器分离进行的。

[0026] 优选地，位置分离是通过使用分离的服务器进行的。

[0027] 优选地，位置分离是通过地理分离进行的。

[0028] 优选地，位置分离是分离的服务器的地理分离，每个服务器保持形成加密数据项的分量部分中的不同分量部分。

[0029] 优选地，位置分离是通过逻辑存储器分离进行的，由此至少一个第一分量部分被存储在第一逻辑存储器中，并且至少一个第二分量部分被存储在第二逻辑存储器中。

[0030] 优选地，位置分离是通过使用分离的服务器进行的，由此至少一个第一分量部分被存储在第一服务器中，并且至少一个第二分量部分被存储在第二服务器中。

[0031] 优选地，位置分离是通过地理分离进行的，由此至少一个第一分量部分被存储在第一地理位置，并且至少一个第二分量部分被存储在第二地理位置，并且其中第一地理位置在地理上与第二地理位置分离。

[0032] 优选地，数据加密步骤包括以下步骤：在对所述数据项进行加密的算法中，使用加密密钥作为参数来对数据项进行加密。

[0033] 优选地，在数据加密步骤之前填充数据项。

[0034] 优选地，加密密钥是对称密钥。

[0035] 优选地，在数学分解步骤之前，通过加密数据项映射步骤对加密数据项进行映射，以形成经映射的加密数据项。

[0036] 优选地，数学分解步骤包括在将加密数据项拆分为分量部分的算法中使用分解密钥作为参数。

[0037] 优选地，分解密钥是质数。

[0038] 优选地，分解密钥是对称密钥。

[0039] 优选地，数据项是参考凭证来存储的。

[0040] 优选地，数据项与实体相关联。

[0041] 优选地，凭证是数据项与实体相关联的实体的实体凭证。

[0042] 优选地，在特定形式中，算法是不可反转的，使得仅拥有算法的变量中的其他变量中的不管哪一个变量是无法获得输入到算法17中的数据项字符串16的。

[0043] 在本发明的又一广泛形式中，提供了一种保护数据项N以用于安全存储数据项的表示的方法，所述数据项具有数据项字符串的形式，所述方法包括以下步骤：

[0044] • 将包含数据项的字符串导入第一环境；

[0045] • 将具有至少一个第一数据项变量的第一函数/算法应用于数据项字符串，从而形成第一修改数据项字符串；

[0046] • 将具有至少一个第二数据项变量的第二函数/算法应用于第一修改字符串，其中第一修改数据项字符串被嵌入第二修改数据项字符串中，所述第二修改数据项字符串具有第一数据项质数的形式；

[0047] • 选择与所述第一数据项质数不同的第二数据项质数；

[0048] • 至少将第一数据项质数定义为关于数据项的数据项私钥；将第一数据项质数和第二数据项质数的乘积定义为关于数据项的数据项公钥；

[0049] • 从第一环境中删除数据项字符串；

[0050] • 维持与第一数据项质数、第一函数/算法和第二函数/算法相关联的数据记录，从而能够通过向第一函数/算法和第二函数/算法提供变量来计算数据项。

[0051] 优选地，变量是数据项公钥。

[0052] 优选地，变量是数据项私钥。

[0053] 优选地，变量是第二数据项变量。

[0054] 优选地，变量是第一数据项变量。

[0055] 优选地，第二数据项变量是数值增量(delta)。

[0056] 优选地，第一数据项变量是ASCII查找表。

[0057] 优选地，第一函数将字符串转换为数字串。

[0058] 优选地，第二函数/算法将数值增量添加到第一修改字符串，以形成第二修改字符串。

[0059] 优选地，在特定形式中，算法是不可反转的，使得仅拥有算法的变量中的其他变量中的不管哪一个变量是无法获得输入到算法17中的数据项字符串16的。

[0060] 在本发明的又一广泛的范围中，提供了一种保护数据项N以用于安全地存储数据项的至少两个表示和至少两个数据项变量的方法，所述数据项N以数据项字符串的形式表示，数据项变量包括至少两个函数的变量，至少两个函数接收数据项的表示作为输入并输出数据项的表示的修改形式，所述方法包括以下步骤：

[0061] • 将数据项字符串导入第一环境；

[0062] • 将具有至少一个第一数据项变量的第一算法应用于数据项字符串，从而形成第一修改数据项字符串；

[0063] • 将具有至少一个第二数据项变量的第二算法应用于第一修改字符串，从而形成第二修改数据项字符串；

[0064] • 从第一环境中删除数据项字符串；

[0065] • 将第一修改数据项字符串、第二修改数据项字符串、第一数据项变量和第二数据项变量中的一个或多个移动到第二环境；

[0066] • 所述第二环境位于与所述第一环境相距较远的位置。

[0067] 优选地，维持数据项字符串、第一函数/算法和第二函数/算法的记录，从而能够通过向第一函数/算法和第二函数/算法提供变量来计算数据项。

[0068] 优选地，变量是数据项公钥。

[0069] 优选地，变量是数据项私钥。

[0070] 优选地，变量是第二数据项变量。

[0071] 优选地，变量是第一数据项变量。

[0072] 优选地，第二数据项变量是数值增量。

[0073] 优选地，第一数据项变量是ASCII查找表。

[0074] 优选地，第一函数将字符串转换为数字串。

[0075] 优选地，第二函数/算法将数值增量添加到第一修改字符串以形成第二修改字符串，由此将第一修改数据项字符串嵌入第二修改数据项字符串中，所述第二修改数据项字符串具有第一数据项质数的形式；选择与所述第一数据项质数不同的第二数据项质数；至少将第一数据项质数定义为关于数据项的数据项私钥；将第一数据项质数和第二数据项质数的乘积定义为关于数据项的数据项公钥。

[0076] 优选地，变量紧邻在其应用到算法之前被动态创建。

[0077] 优选地，每个辅助变量紧邻在其应用到算法之前被动态创建。

[0078] 优选地，辅助变量中的至少一些辅助变量紧邻在其作为算法的输入而应用之前被动态创建。

[0079] 优选地，算法被应用于第一环境20内的数据项字符串。在优选形式中，一旦已经应用了算法，就将变量中的一个或多个变量存储在第二环境21中。

[0080] 优选地，主要变量中的至少一个主要变量被存储在第二环境中。优选地，主要变量中的至少一个主要变量被存储在第二环境中，然后所述至少一个主要变量从第一环境中被删除。

[0081] 优选地，辅助变量中的至少一个辅助变量被存储在第二环境中。在优选的形式中，辅助变量中的至少一个辅助变量被存储在第二环境中，然后所述至少一个辅助变量从第一环境中被删除。

[0082] 优选地，至少一个第一算法14和至少一个第二算法17连续地应用于数据项字符串13。在优选形式中，在将至少一个第一算法14和至少一个第二算法17应用于数据项字符串13之后，至少一个主要变量和至少一个辅助变量被存储在第二环境中。

[0083] 优选地，所述过程被重复N次。

[0084] 优选地，N等于2。

[0085] 优选地，N等于3。

[0086] 优选地，N等于4。

[0087] 优选地，在将至少一个主要变量和至少一个辅助变量存储在第二环境中之后，所述至少一个主要变量和所述至少一个辅助变量从第一环境中被删除。

[0088] 优选地，第二环境21与第一环境20分离。在优选形式中，通过使第二环境位于与第一环境的位置相距较远的位置，第二环境21与第一环境20分离。

[0089] 优选地，第二环境21与第一环境20在逻辑上分离。优选地，存储在第二环境中的那

些输出或变量从第一环境中被删除。

[0090] 优选地，一旦已经应用了算法中的一种或多种算法，包括数据项字符串13在内的数据项11就从第一环境中被删除。

[0091] 优选地，一旦已经应用了算法中的一种或多种算法并且一旦将算法的输出中的一个或多个输出或变量中的一个或多个变量存储在第二环境中，包括数据项字符串13在内的数据项11就从第一环境中被删除。

[0092] 优选地，当期望恢复数据项11中包含的信息12时，反转上述过程。

[0093] 优选地，反转的第一步是将存储在第一环境20和第二环境21中的算法的输出或变量置于一个位置。

[0094] 优选地，变量然后被应用于算法以反转所述过程，由此恢复数据项11以供使用。

[0095] 优选地，在已经使用了数据项11之后，将上述过程重新应用于数据项11，从而再次保护数据项11中包含的信息12达潜在的不确定时间段。

[0096] 优选地，在特定形式中，算法是不可反转的，使得仅拥有算法的变量中的其他变量中的不管哪一个变量是无法获得输入到算法17中的数据项字符串16。

[0097] 在本发明的又一广泛形式中，提供了一种保护数据项N中的信息的方法，所述数据项N以数据项字符串的形式表示，所述方法包括以下步骤：

[0098] • 将数据项字符串导入第一环境；

[0099] • 将具有至少一个第一数据项主要变量和至少一个第一数据项辅助变量的至少一个第一函数/算法应用于数据项字符串，从而形成第一修改数据项字符串；并且其中至少一个第一数据项主要变量包括数据项字符串；

[0100] • 将具有至少一个第二数据项主要变量和至少一个第二数据项辅助变量的第二函数/算法应用于第一修改字符串，从而形成第二修改数据项字符串，并且其中至少一个第二数据项主要变量包括第一修改数据项字符串；

[0101] • 从第一环境中删除数据项字符串；

[0102] • 将变量中的一个或多个变量移动到至少一个第二环境；

[0103] • 所述第二环境位于与所述第一环境相距较远的位置。

[0104] 优选地，用于安全存储数据项的至少两个表示和至少两个数据项变量，数据项变量包括至少两种函数的变量，至少两种函数接收数据项的表示作为输入，并输出数据项的表示的修改形式。

[0105] 优选地，变量包括第一修改数据项字符串、第二修改数据项字符串、第一数据项变量和第二数据项变量中的一个或多个。

[0106] 优选地，在特定形式中，算法是不可反转的，使得仅拥有算法的变量中的其他变量中的不管哪一个变量是无法获得输入到算法17中的数据项字符串16的。

[0107] 优选地，提供了一种数字输入/输出设备，所述数字输入/输出设备包括用于实现如上所述的方法的装置。

[0108] 优选地，设备被实现为智能电话上的软件应用。

[0109] 优选地，提供了一种存储有代码的介质，当由处理器执行代码时，代码实现上述方法。

[0110] 优选地，介质是非暂时性介质。

[0111] 优选地，提供了一种数字输入/输出设备，所述数字输入/输出设备包括用于基于上述方法来识别准备传输数据项的物理特征的装置。

[0112] 优选地，设备被实现为智能电话上的软件应用。

[0113] 在本发明的又一广泛形式中，提供了一种对至少具有第一存储位置和第二存储位置的系统中的安全入侵做出响应的方法，所述系统实现一种加密并存储数据项的方法，所述方法包括：

[0114] a.数据加密步骤，其中将数据项加密以形成加密数据项；

[0115] b.数学分解步骤，其中将加密数据项在数学上分解为包括至少一个第一分量部分和至少一个第二分量部分在内的两个或更多个加密数据项分量部分；

[0116] c.将分量部分中的至少一个分量部分存储在第一存储位置，并且将第二分量部分存储在与分量部分中的其他分量部分分离的第二存储位置，所述方法包括：

[0117] 如果在第一位置检测到安全入侵，使得至少一个第一分量部分受到损害：

[0118] 从第一位置删除至少一个第一分量部分；以及

[0119] 从第二位置删除至少一个第二分量部分。

[0120] 在本发明的又一广泛形式中，提供了一种分布式加密系统，其中，

[0121] a.将要加密的数据放置在主服务器上，然后对要加密的数据进行扩展和混淆以形成混淆串；

[0122] b.然后使用对称加密密钥对混淆串进行加密，以形成加密串；

[0123] c.然后将打包数据的串逐步添加到加密串，直到得到的数据串在计算上等同于最接近的质数，然后将所述最接近的质数定义为初始质数；

[0124] d.生成相似长度的附加质数，并且利用预定的公钥算法，使用初始质数和附加质数来生成公钥。

[0125] 优选地，初始质数从存储器中被删除并且未被存储。

[0126] 优选地，所得的分量然后被存储在不同的位置。

[0127] 优选地，对称加密密钥和打包数据的串被存储在主服务器上，公钥被存储在辅助服务器上，并且附加质数被存储在第三服务器上。

[0128] 优选地，当要对数据解密时，

[0129] a.从相应的服务器中检索公钥和附加质数；

[0130] b.利用预定公钥算法，将公钥与附加质数结合使用，以计算初始质数；

[0131] c.然后从所得的质数中减去所存储的打包数据的串，并使用主服务器上存储的对称加密密钥对所得的加密串进行解密；以及

[0132] d.使用反向的最初用于原始混淆数据的混淆规则，根据所得的扩展混淆数据串对期望目标数据进行去混淆。

[0133] 优选地，系统使用任何形式的公钥加密，包括但不限于RSA或Shamir算法。

[0134] 在本发明的又一广泛形式中，提供了一种数据保护方法，所述方法包括以下步骤：

[0135] a.用对称密钥对要加密的数据进行加密；

[0136] b.混淆并扩展对称密钥；

[0137] c.然后使用第二对称密钥对经混淆并扩展的对称密钥进行加密，然后将第二对称密钥存储在主服务器上；

[0138] d.然后将打包数据的串添加到加密对称密钥以形成质数；

[0139] e.生成相似长度的第二质数，并且两个质数。

[0140] 优选地，对称加密密钥和打包数据的串被存储在主服务器上，公钥被存储在辅助服务器上，并且附加质数被存储在第三服务器上。

[0141] 优选地，通过反转所述步骤来执行数据的解密。

附图说明

[0142] 现在将参考附图描述本发明的实施例，其中：

[0143] 图1A、图1B、图1C和图1D是本发明的系统的一般实施例的应用阶段的框图，

[0144] 图2是至少执行本发明的系统的第一实施例的步骤的流程图，

[0145] 图3是根据本发明的系统的适合于实现图2的第一实施例的步骤以存储和随后检索数据项的主要组件的框图，

[0146] 图4是至少执行本发明的系统的第二实施例的步骤的流程图，

[0147] 图5是概述图4的第二实施例的至少一个示例的存储和检索步骤的过程图，其中数据项包括短数据串，

[0148] 图6是概述图4的第二实施例的至少一个示例的存储和检索步骤的过程图，其中数据项包括长数据串，

[0149] 图7是适用于系统的任何实施例的使用场景的框图系统图。

具体实施方式

[0150] 广泛地，在一个实施例中，公开了一种加密并存储数据项的方法；所述方法包括：

[0151] 数据加密步骤，其中将数据项加密以形成加密数据项；

[0152] 数学分解步骤，其中将加密数据项在数学上分解为包括至少一个第一分量部分和至少一个第二分量部分在内的两个或更多个加密数据项分量部分；

[0153] 将分量部分中的至少一个分量部分存储在与分量部分中的其他分量部分分离的位置。

[0154] 在优选形式中，位置分离是通过逻辑存储器分离进行的，由此至少一个第一分量部分被存储在第一逻辑存储器中，并且至少一个第二分量部分被存储在第二逻辑存储器中。

[0155] 在备选的优选形式中，位置分离是通过使用分离的服务器进行的，由此至少一个第一分量部分被存储在第一服务器中，并且至少一个第二分量部分被存储在第二服务器中。

[0156] 在特别优选的形式中，位置分离是通过地理分离进行的，由此至少一个第一分量部分被存储在第一地理位置，并且至少一个第二分量部分被存储在第二地理位置，并且其中第一地理位置在地理上与第二地理位置分离。

[0157] 在又一特定形式中，位置分离是分离的服务器的地理分离，每个服务器保持形成加密数据项的分量部分中的不同分量部分。

[0158] 广泛地在另一实施例中，公开了一种保护数据项N以用于安全存储数据项的表示的方法，所述数据项具有数据项字符串的形式，所述方法包括以下步骤：

[0159] 将包括数据项的字符串导入第一环境；

[0160] 将具有至少一个第一数据项变量的第一算法应用于数据项字符串，从而形成第一修改数据项字符串；

[0161] 将具有至少一个第二数据项变量的第二算法应用于第一修改字符串，由此将第一修改数据项字符串嵌入第二修改数据项字符串中，所述第二修改数据项字符串具有第一数据项质数的形式；

[0162] 选择与所述第一数据项质数不同的第二数据项质数；

[0163] 至少将第一数据项质数定义为关于该数据项的数据项私钥；将第一数据项质数和第二数据项质数的乘积定义为关于该数据项的数据项公钥；

[0164] 从第一环境中删除数据项字符串；

[0165] 维持与第一数据项质数、第一算法和第二算法相关联的数据记录，从而可以通过向第一算法和第二算法提供变量来计算数据项。

[0166] 在优选形式中，变量是数据项公钥。

[0167] 在备选的优选形式中，变量是数据项私钥。

[0168] 在备选的优选形式中，变量是第二数据项变量。

[0169] 在备选的优选形式中，变量是第一数据项变量。

[0170] 在备选的优选形式中，第二数据项变量是数值增量。

[0171] 在备选的优选形式中，第一数据项变量是ASCII查找表。

[0172] 在备选的优选形式中，第一算法将字符串转换为数字串。

[0173] 在备选的优选形式中，第二算法将数值增量添加到第一修改字符串，以形成第二修改字符串。

[0174] 在特别优选的形式中，由于第二环境位于与第一环境的位置相距较远的位置，因此第二环境21与第一环境20分离。

[0175] 在另一特别优选的形式中，第二环境21与第一环境20在逻辑上分离。

[0176] 参考图1A、图1B、图1C和图1D，本发明的系统10的优选实施例试图保护数据项11，以安全地存储包含在数据项11中的信息12。

[0177] 在优选形式中，数据项11为数据项字符串13的形式。在优选形式中，至少一个第一算法14被应用于数据项字符串13，从而产生第一修改数据项字符串16，作为至少一个第一算法14的输出。优选地，第一算法14是数学函数的形式，该数学函数具有至少一个第一数据项主要变量13A并且具有至少一个第一数据项辅助变量15。在优选形式中，第一数据项主要变量13A是数据项字符串13。

[0178] 在优选形式中，至少一个第二算法17被应用于数据项字符串13，从而产生第二修改数据项字符串19，作为至少一个第二算法17的输出。优选地，第二算法17为数学函数的形式，该数学函数具有至少一个第二数据项主要变量16A并且具有至少一个第二数据项辅助变量18。在优选形式中，第二数据项主要变量16A是第一修改数据项字符串16，(也就是说，在应用至少一个第二算法17之前已通过应用算法对数据项字符串13进行了修改之后的数据项字符串13)。在这种情况下，已经通过应用至少一个第一算法14对数据项字符串13进行了修改，该至少一个第一算法14应用于数据项字符串13。

[0179] 在优选形式中，变量紧邻在其应用到算法之前被动态创建。

[0180] 在优选形式中，每个辅助变量紧邻在其应用到算法之前被动态创建。

[0181] 在优选形式中，至少一些辅助变量紧邻在其作为算法的输入而应用之前被动态创建。

[0182] 在优选形式中，将算法应用于第一环境20内的数据项字符串。在优选形式中，一旦已应用了算法，就将一个或多个变量存储在第二环境21中。

[0183] 在优选形式中，将主要变量中的至少一个主要变量存储在第二环境中。在优选形式中，将主要变量中的至少一个主要变量存储在第二环境中，并且然后从第一环境中将其删除。

[0184] 在优选形式中，将辅助变量中的至少一个存储在第二环境中。在优选形式中，将辅助变量中的至少一个存储在第二环境中，并且然后从第一环境中将其删除。

[0185] 在优选形式中，将至少一个第一算法14和第二算法17连续地应用于数据项字符串13。在优选形式中，在将至少一个第一算法14和至少一个第二算法17应用于数据项字符串13之后，将至少一个主要变量和至少一个辅助变量存储在第二环境中。

[0186] 可以重复紧接以上描述的过程。

[0187] 在优选形式中，在将至少一个主要变量和至少一个辅助变量存储在第二环境中之后，将所述至少一个主要变量和所述至少一个辅助变量从第一环境中删除。

[0188] 在优选形式中，第二环境21与第一环境20分离。在优选形式中，由于第二环境位于与第一环境的位置相距较远的位置，所以第二环境21与第一环境20分离。

[0189] 在优选形式中，第二环境21与第一环境20在逻辑上分离。优选地，然后从第一环境中删除存储在第二环境中的那些输出或变量。

[0190] 优选地，一旦已经应用一种或多种算法，就从第一环境中删除包括数据项字符串13的数据项11。

[0191] 优选地，一旦已经应用一种或多种算法并且一旦将算法的一个或多个输出或一个或多个变量存储在第二环境21中，就从第一环境中删除包括数据项字符串13的数据项11。

[0192] 当期望恢复包含在数据项11中的信息12时，反转上述过程。反转的第一步是将存储在第一环境20和第二环境21中的算法的输出或变量置于一个位置。然后将变量应用于算法以反转过程，从而恢复数据项11以供使用。

[0193] 在一些实施例中，在已经使用了数据项11之后，将上述过程重新应用于数据项11，从而再次保护数据项11中包含的信息12达潜在不确定的时间段。

[0194] 要注意的是，将要描述的实施例不仅仅是具有分布的“密钥”的更高级别的加密。使用算法将数据解构和重新创建，算法该在算法可以进行处理之前需要将存储的几项分隔的信息汇集在一起。

[0195] 参考图1D，任何给定的算法14、17可以产生多于一个的输出，在这种情况下为输出E、F。这可以根据使用的算法的性质而产生。下面描述的第二实施例包括可以产生这种形式的输出的Shamir算法的应用。

[0196] 在特定形式中，算法使得仅拥有E或F或D中的不管哪一个是无法获得输入到算法17中的数据项字符串16的。

[0197] 在给出的示例中，应用了第一算法和第二算法。可以应用附加算法来形成更长的序列，如图1D中的附加算法22、23所示。

[0198] 第一优选实施例

[0199] 参考图2,公开了根据第一优选实施例的保护数据项以用于安全存储数据项的表示的方法的流程图,所述数据项具有数据项字符串的形式,所述方法包括以下步骤:

[0200] • 将包含数据项在内的字符串导入第一环境;

[0201] • 将具有至少一个第一数据项变量的第一函数/算法应用于数据项字符串,从而形成第一修改数据项字符串;

[0202] • 将具有至少一个第二数据项变量的第二函数/算法应用于第一修改字符串,由此将第一修改数据项字符串嵌入第二修改数据项字符串中;所述第二修改数据项字符串具有第一数据项质数的形式;

[0203] • 选择与所述第一数据项质数不同的第二数据项质数;

[0204] • 至少将第一数据项质数定义为关于该数据项的数据项私钥;将第一数据项质数和第二数据项质数的乘积定义为关于该数据项的数据项公钥;

[0205] • 从第一环境中删除数据项字符串;

[0206] • 维持与第一数据项质数、第一函数/算法和第二函数/算法相关联的数据记录,从而可以通过向第一函数/算法和第二函数/算法提供变量来计算数据项。

[0207] 优选地,变量是数据项公钥。

[0208] 优选地,变量是数据项私钥。

[0209] 优选地,变量是第二数据项变量。

[0210] 优选地,变量是第一数据项变量。

[0211] 优选地,第二数据项变量是数值增量。

[0212] 优选地,第一数据项变量是ASCII查找表。

[0213] 优选地,第一函数将字符串转换为数字串。

[0214] 优选地,第二函数/算法将数值增量添加到第一修改字符串,以形成第二修改字符串。

[0215] 参考图3,公开了第一优选实施例的实施方式。通常,以待保护的数据项字符串120的形式的数据来自诸如客户端设备110之类的源,并且在这种情况下通过诸如互联网111之类的公共网络以主处理服务器112的形式到达第一环境20。随后,主处理服务器112以优选的形式对数据项字符串120进行加密以形成加密数据项字符串113。然后,将第一算法14应用于加密数据项字符串113。第一算法14找到数字上紧邻在加密数据项字符串113的数值之上的下一个可用的质数114。第一算法14将该质数114作为第一修改数据项字符串16进行输出。在这种情况下,第一算法14已用于混淆加密数据项字符串113。接下来,使用本领域中已知的公钥算法生成辅助质数15。

[0216] 将辅助质数15和用于加密要保护的数据的加密密钥19存储在主处理服务器12上。使用本领域中已知的公钥技术将初始质数14和辅助质数15组合以产生公钥,然后将其与加密数据13和初始质数14之间的差异18一起存储17在远程服务器16上。

[0217] 在确认分量17、18存储在辅助服务器16上之后,将包含在质数14中的原始加密数据13从存储器中删除。

[0218] 当请求解密受保护的数据时,辅助服务器16用于将公钥17与差异18一起发送给用于去混淆和解密的主服务器12。在主服务器12处,将存储的质数15应用于公钥17以检索初

始质数14。然后将差异18应用于初始质数14，从而生成加密的原始数据集13。然后使用本地存储的加密密钥19将受保护的数据解密为其未加密状态21。

[0219] 在示例实施例中，主服务器用于存储要保护的数据的加密密钥以及以后在去混淆处理中使用的辅助质数。辅助服务器用于存储从初始质数和辅助质数生成的公钥以及第一质数与数据加密状态下的数据之间的差异。备选实施例可以看到存储在任意数量的远程服务器上的任何可访问位置处的任何密钥分量，只要可以检索到这些分量即可。

[0220] 第二优选实施例

[0221] 参考图4，示出了执行本发明的系统的至少第二实施例的步骤的流程图。具体的实现步骤在图5和图6中进一步说明。

[0222] 重要的是要注意，后面的解决方案不仅是使用分布式的“密钥”的更高级别的加密，而且还使用算法对数据进行解构和重新创建，该算法需要在算法可以进行处理之前将存储的几项分隔的信息汇集在一起。

[0223] 示例实施例使用公钥加密技术来混淆并允许用于以后重新编译和解密的密钥分量的安全分布。备选实施例可以使用非公开密钥加密系统，例如，本领域已知的Shamir密钥共享算法。在该备选实施例中，加密的数据仍然具有应用于该加密的数据的质数但不是使用公钥方法生成辅助质数，将质数作为盐应用于加密的数据以在数学线上产生随机点。在该模型中，需要至少两个位置来分布随机点。因此，位置被存储在分离的服务器上，并且盐被存储在服务器之一上。在又一备选实施例中，可以将无限数量的随机点存储在无限数量的位置上。

[0224] 示例1-小型数据加密

[0225] 参考图5：当要加密的数据的长度小于200个字符时，使用小型数据加密方法。选择该数字以允许在加密之前对数据进行充分的随机填充，并且还确保所生成的质数不会太大而不会影响创建时间。

[0226] 为了创建加密的分布式安全数据：

[0227] 用户将输入数据项11，输入数据项11包括用户名(U1)、保管库(vault)名称(VN1)、未加密凭证(credentials)(UC1)(例如信用卡号)、交易类型(TT1)和交易参考(TR1)，数据项11中的至少一项包括要保护的信息12。在这种情况下，信息12在未加密凭证13(UC1)内。

[0228] 在这种情况下，系统将生成一个或多个变量15、18，该一个或多个变量15、18包括随机保管库ID(ID1)、质数(P1)和对称密钥(K1)，随机保管库ID(ID1)、质数(P1)和对称密钥(K1)中的至少一些将用作用于对信息12进行连续操作的至少一个第一算法或函数14和至少一个第二算法或函数17的变量。

[0229] 系统将以预定顺序执行算法或函数14、17，在这种情况下包括首先用随机数据(作为变量)填充未加密凭证13(UC1)，以创建填充的未加密凭证(PUC1)。

[0230] 然后，在这种情况下，系统将至少一个第二算法17应用于加密算法，以便在这种情况下以对称密钥(K1)的形式用至少一个第二数据项变量18来对填充的未加密凭证(PUC1)进行加密，以创建加密串(ES1)。

[0231] 在这种情况下，应用了又一个函数或算法，由此将通过ASCII转换表(用作映射函数的变量)将加密串(ES1)转换或映射为大整数(LI1)。

[0232] 在这种情况下，应用又一个函数或算法，由此系统将使用质数(P1)作为变量，并且

使用算法将大整数(LI1)拆分为两个或更多个部分(SP1...n)。在一种形式中,该函数基于Shamir算法。

[0233] 然后,系统将函数或算法的变量和输出中的一个或多个分离到分离的远程位置。在该特定实例中,系统将在数据库存储区内存储保管库ID(ID1)、第一部分(SP1)和对称密钥(K1)以及质数(P1)。

[0234] 系统将把ID(ID1)、其余部分(SP2...n)返回到不同的位置。

[0235] 为了从加密的分布式系统中检索数据:

[0236] 用户将提交ID(ID1)、交易类型(TT1)、部分(SP2...n);

[0237] 系统将通过用户提供的保管库ID(ID1)来检索质数1(P1)、部分1(SP1)和对称密钥(K1);

[0238] 系统将使用(P1)和部分(SP1...n)来重建大整数(LI1);

[0239] 将通过ASCII转换表将大整数(LI1)转换为加密串(ES1);

[0240] 系统将使用对称密钥(K1)解密为填充的未加密凭证(PUC1);

[0241] 系统将移除填充以产生未加密凭证(UC1);

[0242] 系统将检查交易类型(TT1),以确定是否应生成另一个脱机保管库;

[0243] 未加密凭证(UC1)将与另一个脱机保管库(如果适用)一起返回给用户。

[0244] 示例2-大型数据加密

[0245] 参考图6:当要加密的数据的长度大于200个字符时,使用大型数据加密方法。系统根据传递的未加密凭证自动确定要使用哪种方法。

[0246] 为了创建加密的分布式安全数据:

[0247] 用户将输入用户名(U1)、保管库名称(VN1)、未加密凭证(UC1)(例如照片)、交易类型(TT1)和交易参考(TR1);

[0248] 系统将生成随机保管库ID(ID1)、质数(P1)、两个对称密钥(K1)(K2);

[0249] 系统将确定未加密凭证(UC1)是大类型的。

[0250] 系统将使用对称密钥(K1)对未加密凭证(UC1)进行加密,以创建加密数据(ED1);

[0251] 系统将加密数据(ED1)拆分成两个部分,即前100个字节(FBD1)和其余部分(RBD1);

[0252] 系统将用随机数据填充对称密钥(K1),以创建填充的未加密密钥(PUK1);

[0253] 系统将使用对称密钥(K2)对填充的未加密密钥(PUK1)进行加密,以创建加密串(ES1);

[0254] 加密串(ES1)将通过ASCII转换表被转换为大整数(LI1);

[0255] 系统将使用质数(P1)和算法将大整数(LI1)拆分为两个或更多个部分(SP1...n);

[0256] 系统将在数据库存储区内存储保管库ID(ID1)、第一部分(SP1)和对称密钥(K2)、质数(P1)以及其余数据字节(RBD1);

[0257] 系统将返回保管库ID(ID1)、其余部分(SP2...n)和数据的第一个字节(FBD1)。

[0258] 为了从加密的分布式系统中检索数据:

[0259] 用户将提交保管库ID(ID1)、交易类型(TT1)、部分(SP2...n)和数据的第一字节(FBD1);

[0260] 系统将通过用户提供的保管库ID(ID1)来检索质数1(P1)、部分1(SP1)、对称密钥

(K2)和其余数据字节(RBD1)；

[0261] 系统将使用(P1)和部分(SP1...n)来重建大整数(LI1)；

[0262] 大整数(LI1)将通过ASCII转换表被转换为加密串(ES1)；

[0263] 系统将使用对称密钥(K2)解密为填充的未加密密钥(PUK1)；

[0264] 系统将移除填充以产生未加密密钥(K1)；

[0265] 系统将数据的第一字节(FBD1)与数据的其余字节(RBD1)合并以创建加密数据(ED1)；

[0266] 系统将对加密数据(ED1)使用未加密密钥(K1)以产生未加密凭证(UC1)；

[0267] 系统将检查交易类型(TT1)，以确定是否应生成另一个脱机保管库；

[0268] 未加密凭证(UC1)将与另一个脱机保管库(如果适用)一起返回给用户。

[0269] 使用例

[0270] 图7是适用于系统的任何实施例的使用场景的系统框图。

[0271] 在这种情况下，用户201为了接收商品或服务的目的向实体203提供信用卡详细信息202。在实体203可能要求再次或在将来的某个时间访问信用卡详细信息202的情况下，实体203可以登记(enlist)本申请的系统10以保护信用卡详细信息202。为了做到这一点，该实体203可以使信用卡详细信息202经过上述一个或多个实施例的算法14、17和安全处理，从而使变量202A和202B分别存储在分离的位置206和207中。一旦完成安全处理，就可以完全删除信用卡详细信息202。

[0272] 如果实体203希望恢复信用卡详细信息202，以便例如利用它们来触发由用户201授权的对实体203的定期支付，则实体203将变量202A和202B置于计算环境204，从而重新创建信用卡详细信息202，并且在这种情况下，使之触发在计算环境204处的脱机交易或“无卡”交易，从而使资金205从用户帐户201A转移到实体帐户203A。

[0273] 在一些情况下，计算环境204可以是其中已存储有变量202A或202B的环境206、207。在备选形式中，计算环境信息204可以是完全独立的环境。在一个示例中，完全独立的环境可以是EFTPOS终端。在备选形式中，计算环境204可以是分布式计算环境。

[0274] 在环境违规的情况下采取的行动

[0275] 如果确定环境已经受到损害-例如，如果确定已获得对环境206中的变量202A或环境207中的变量202B的未授权访问，则优选程序是鼓励删除在尚未被确定为受到损害的环境中的变量。以这种方式，仅从来自受损害环境的变量来重建信用卡详细信息202变得极其困难。

[0276] 在特定形式中，可以选择算法14、17，使得在没有相应的辅助变量的情况下，由算法输出的变量在任何情况下都不能反转。

[0277] 备选实施例

[0278] 在示例实施例中，要加密的数据的源是客户端设备，例如移动电话。在备选实施例中，源数据可以来自任何地方。

[0279] 在所有这些备选实施例中，可以使用初始数据的附加填充来进一步扩展混淆选项。

[0280] 在已经描述的备选实施例中，要保护的数据通常小于300字节。这种大小的质数的生成相对容易，但随着数据大小增加超过300字节而变得更难。备选实施例可以将已经描述

的过程应用于初始加密数据的子集。理想情况下，子集在数据中的大小和位置应使其与蛮力攻击一样费力。

[0281] 在又一备选实施例中，大型数据块可以被分解成多个部分，并且可以应用相同的技术。

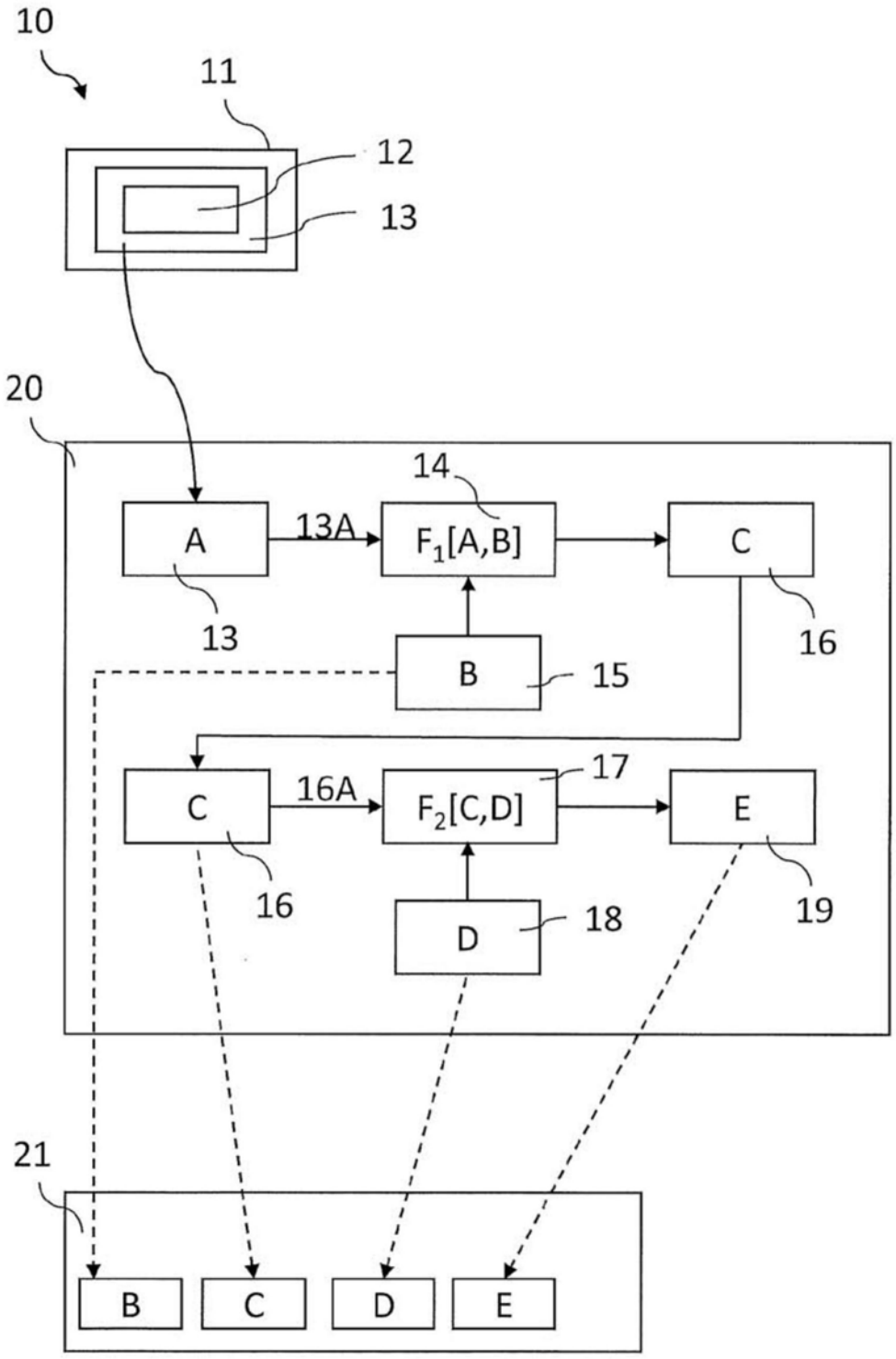

10
11
12
13
20
14
A
13A
F_1[A,B]
C
13
16
B
15
C
16A
F_2[C,D]
17
E
16
19
D
18
21
B
C
D
E

图1A

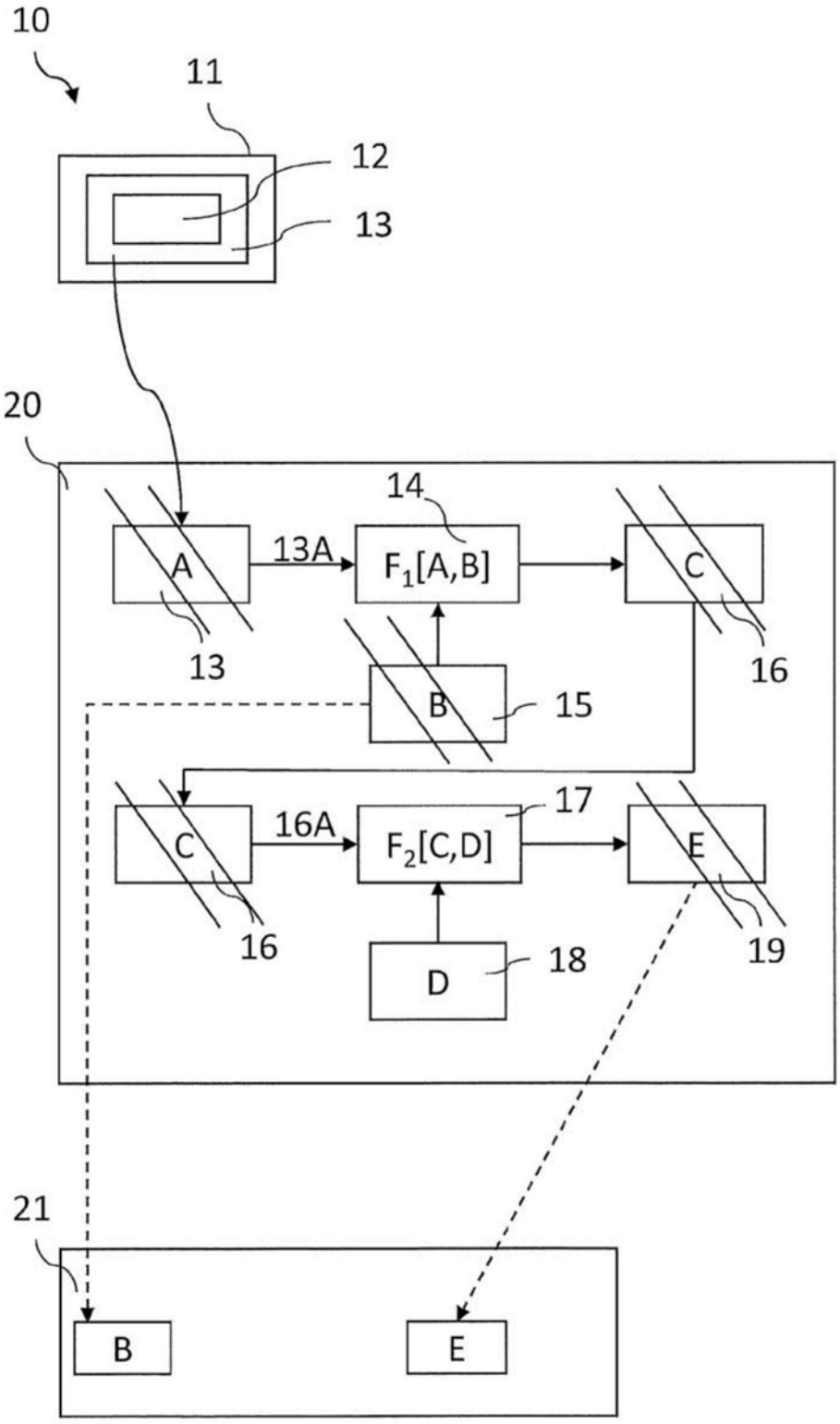

10
11
12
13
20
14
A
13A
F_1[A,B]
C
13
16
B
15
C
16A
F_2[C,D]
17
E
16
19
D
18
21
B
E

图1B

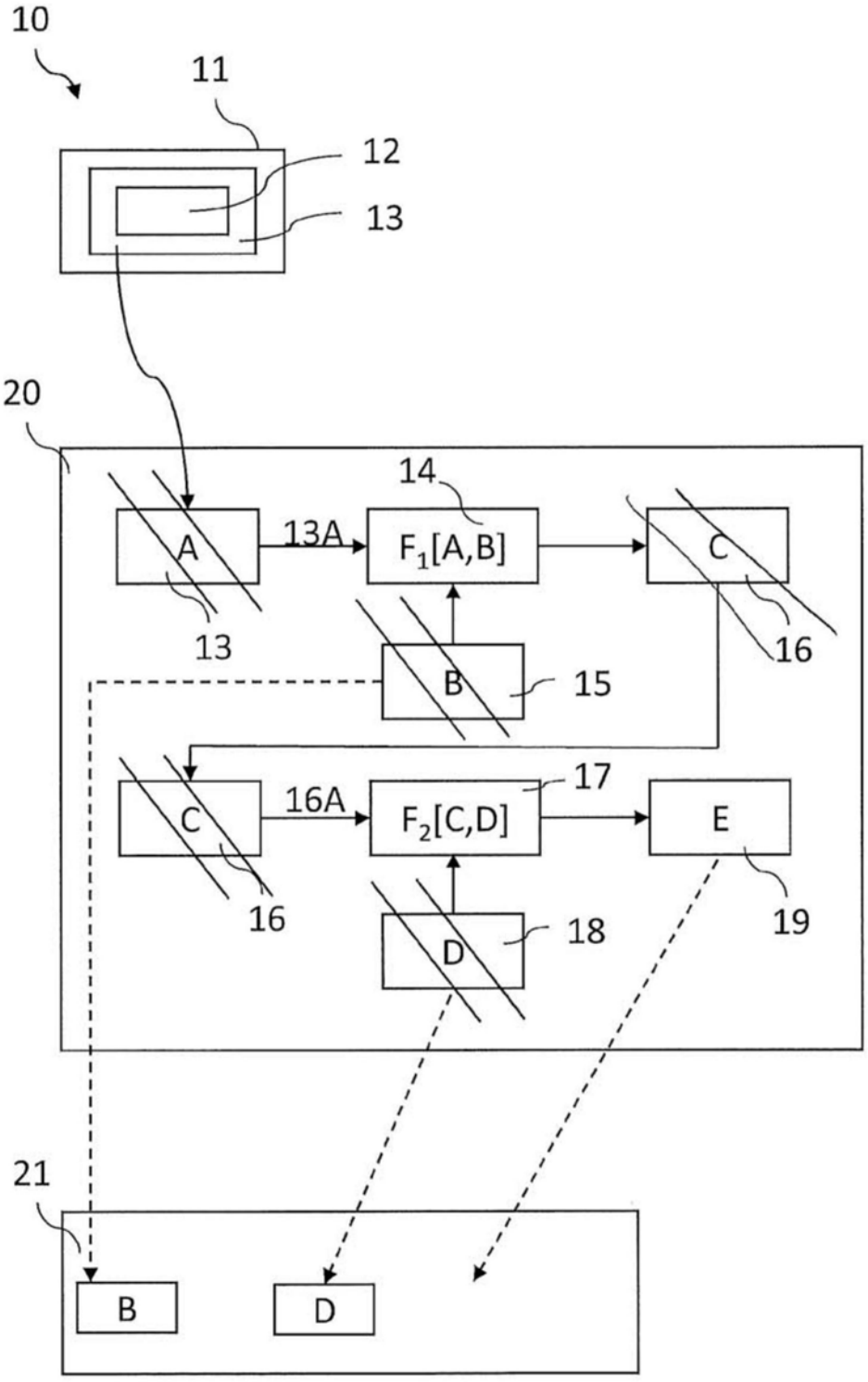

10
11
12
13
20
14
A
13A
F_1[A,B]
C
13
16
B
15
C
16A
17
F_2[C,D]
E
16
19
D
18
21
B
D

图1C

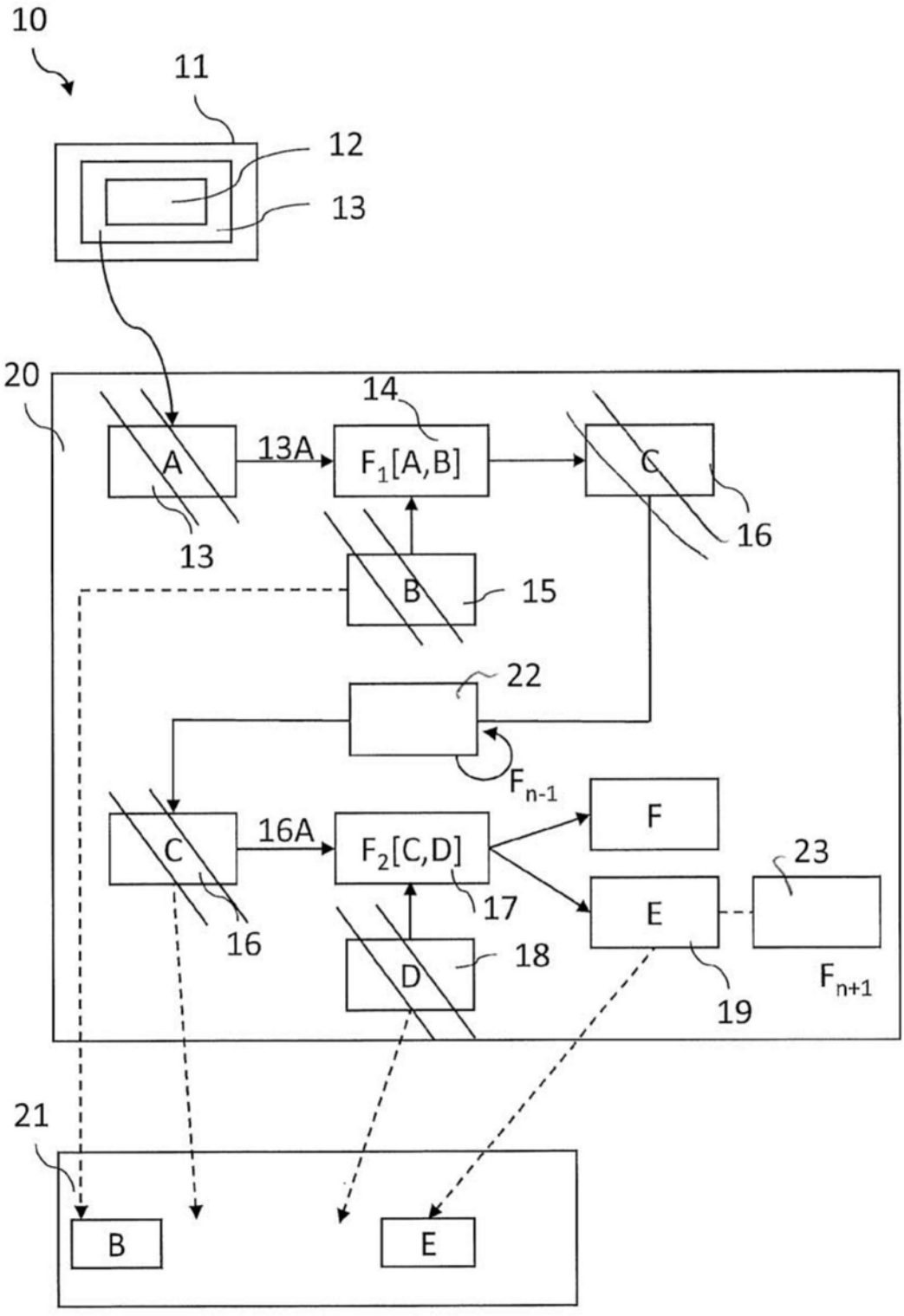

10
11
12
13
20
14
A
13A
F_1[A,B]
C
16
13
B
15
22
F_{n-1}
C
16A
F_2[C,D]
F
23
E
17
16
D
18
F_{n+1}
19
21
B
E

图1D

流程图

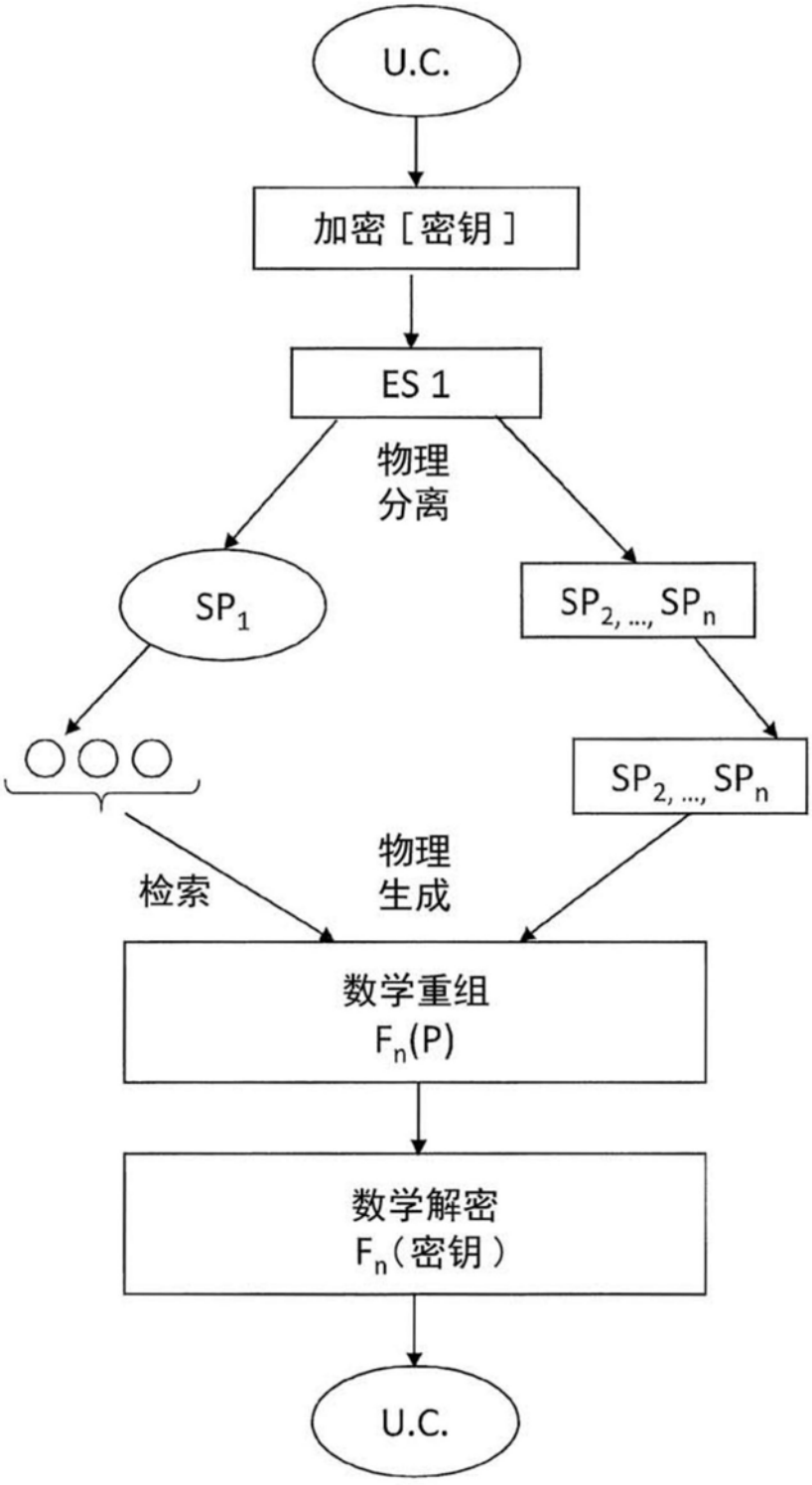

U.C.
加密［密钥］
ES 1
物理
分离
SP1
SP2, ..., SPn
SP2, ..., SPn
检索
物理
生成
数学重组
Fn(P)
数学解密
Fn（密钥）
U.C.

图2

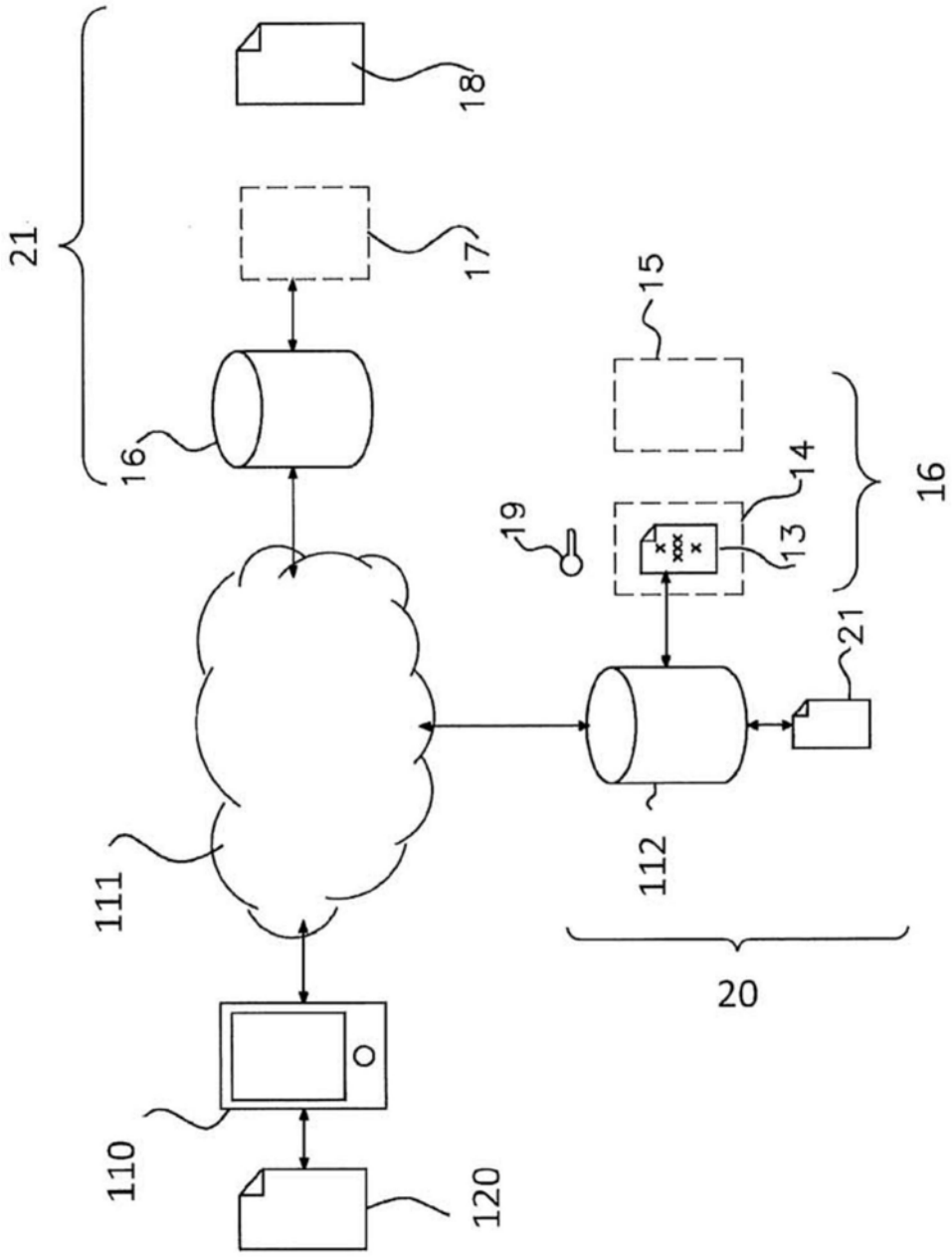


图3

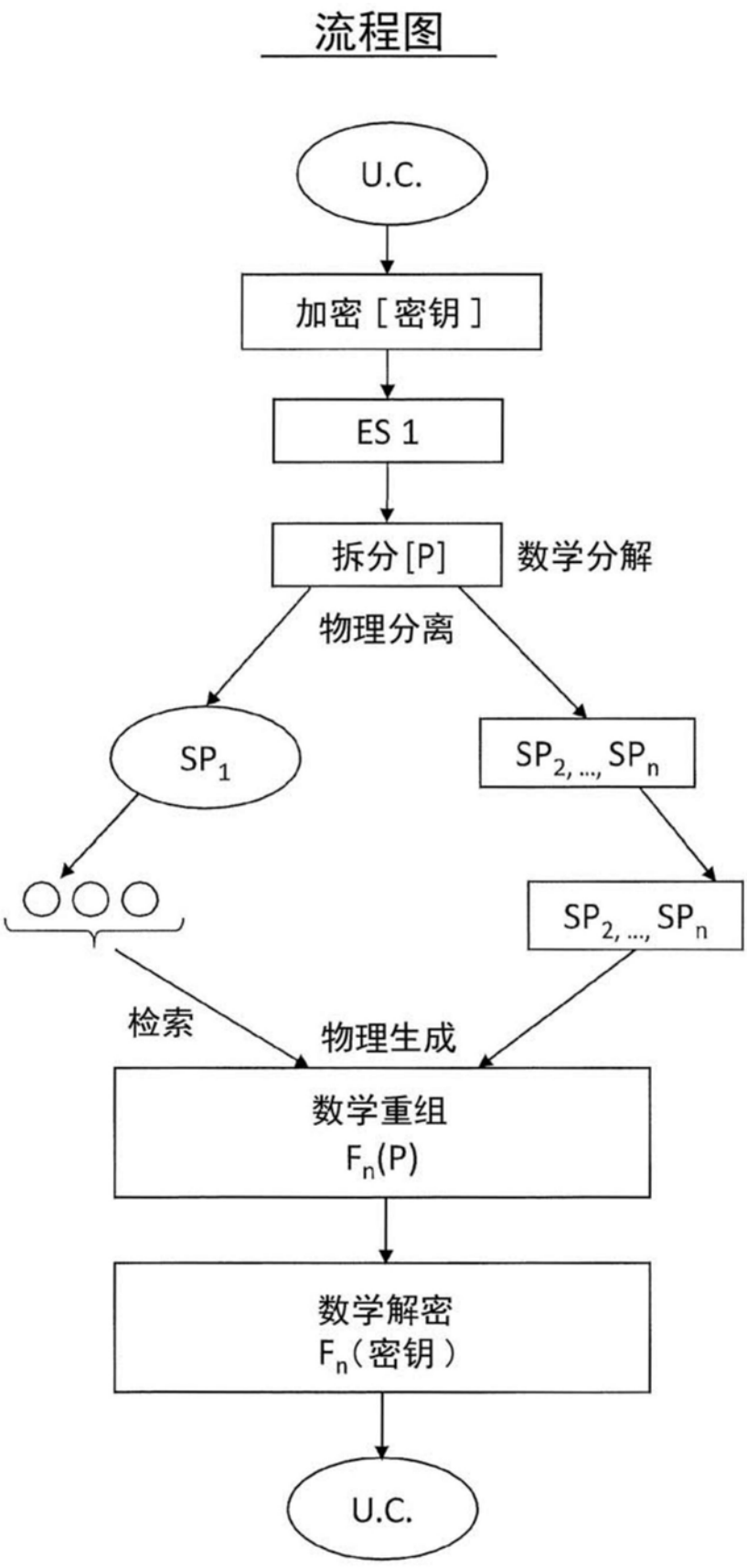

流程图
U.C.
加密 [密钥]
ES 1
拆分 [P]
数学分解
物理分离
SP1
SP2, ..., SPn
SP2, ..., SPn
检索
物理生成
数学重组
Fn(P)
数学解密
Fn(密钥)
U.C.

图4

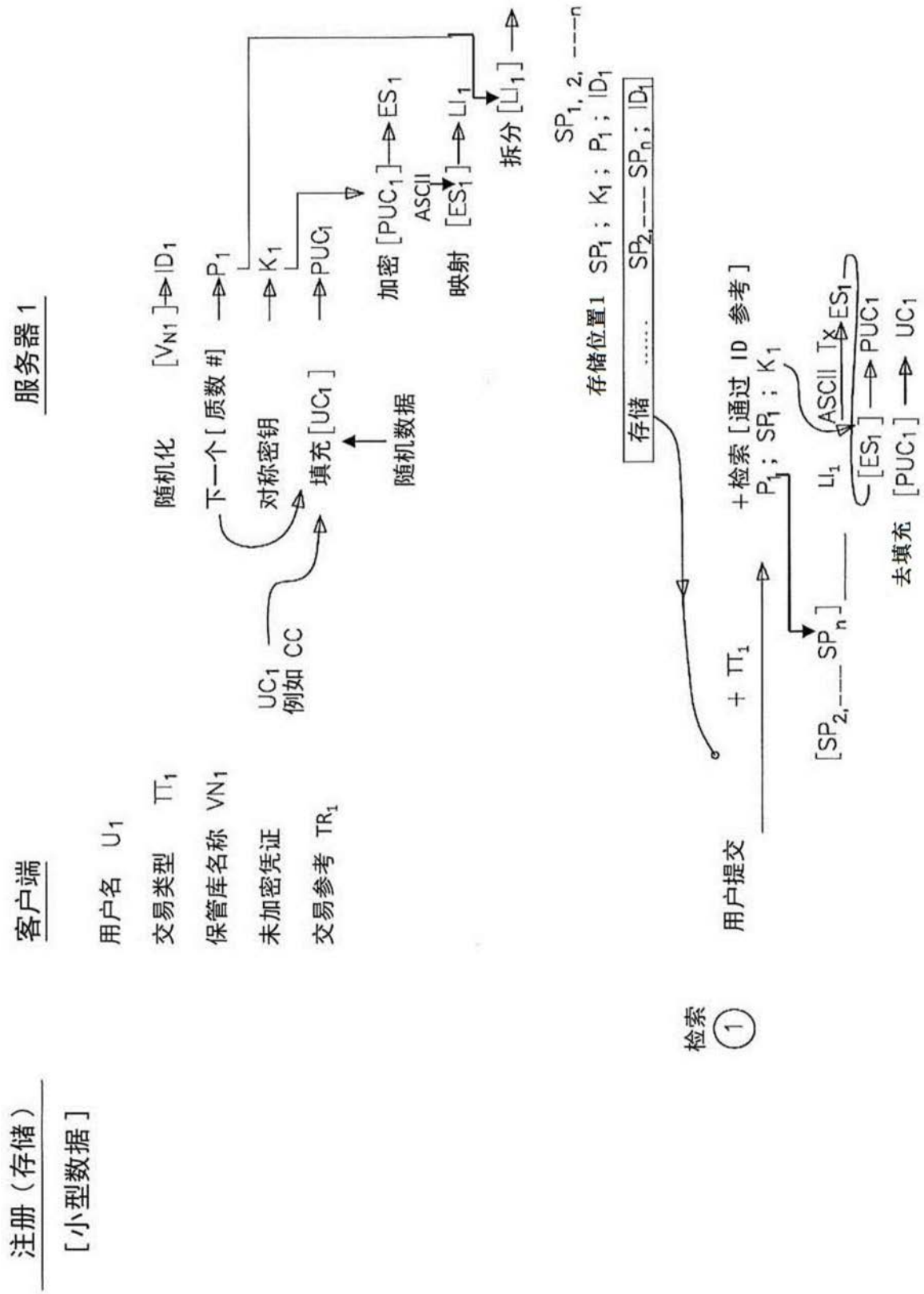

注册（存储）
[小型数据]
客户端
用户名 U_1
交易类型 TT_1
保管库名称 VN_1
未加密凭证
交易参考 TR_1
服务器 1
随机化 $[V_{N1}] \rightarrow ID_1$
下一个[质数#] $\rightarrow P_1$
对称密钥 $\rightarrow K_1$
填充 $[UC_1]$ $\rightarrow PUC_1$
随机数据
UC_1 例如 CC
加密 $[PUC_1] \rightarrow ES_1$
ASCII
映射 $[ES_1] \rightarrow LI_1$
拆分 $[LI_1] \rightarrow$
$SP_{1,2,---n}$
存储位置1 SP_1 ; K_1 ; P_1 ; ID_1
存储 ..... $SP_{2,---}$ SP_n ; ID_1
检索 ①
用户提交
$+ TT_1$
+检索[通过 ID 参考]
P_1 ; SP_1 ; K_1
$[SP_{2,---}$ $SP_n]$
LI_1
ASCII
$[ES_1] \rightarrow PUC_1$
去填充 $[PUC_1] \rightarrow UC_1$

图5

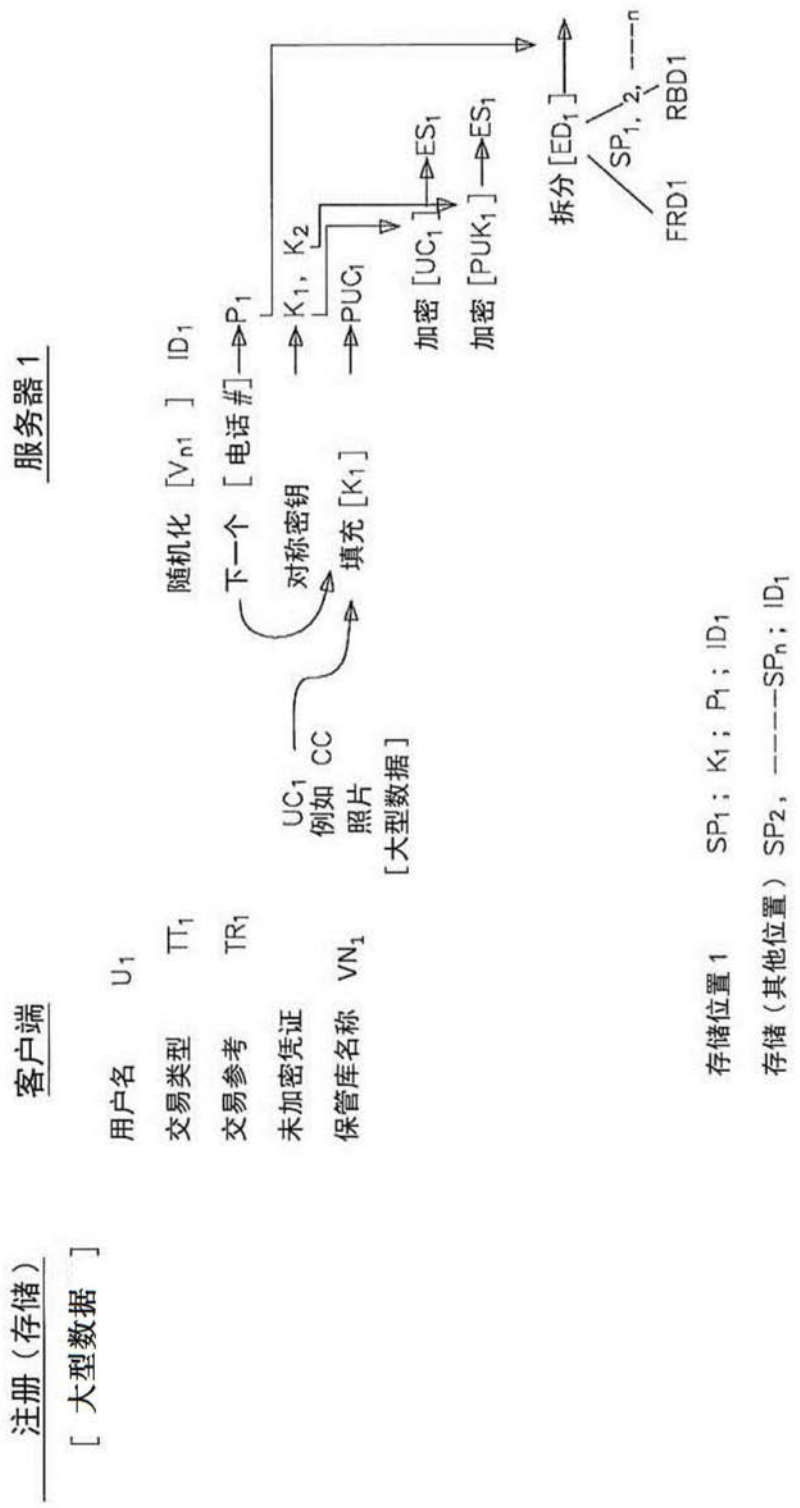

服务器 1
客户端
注册（存储）
[大型数据]
用户名 U_1
交易类型 TT_1
交易参考 TR_1
未加密凭证
保管库名称 VN_1
随机化 [V_{n1}] ID_1
下一个 [电话 #] → P_1
对称密钥 → K_1, K_2
填充 [K_1] → PUC_1
UC_1 例如 CC 照片 [大型数据]
加密 [UC_1] → ES_1
加密 [PUK_1] → ES_1
拆分 [ED_1]
SP_1, 2, ---n
FRD1 RBD1
存储位置 1 SP_1 ; K_1 ; P_1 ; ID_1
存储（其他位置） SP_2, ----SP_n ; ID_1

图6

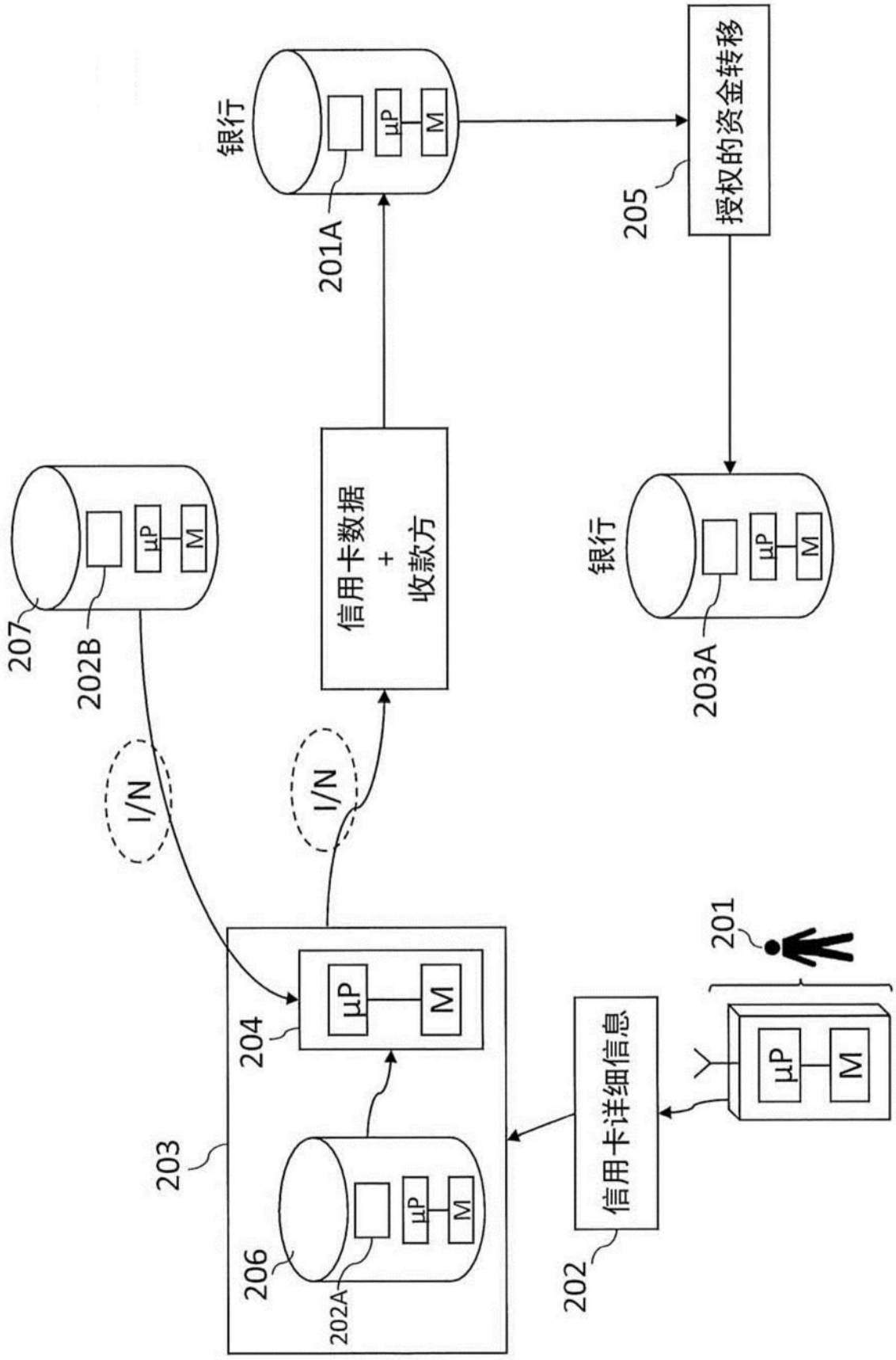

银行
μP
M
201A
205
授权的资金转移
信用卡数据
+
收款方
207
202B
I/N
I/N
银行
203A
201
204
203
206
202A
信用卡详细信息
202

图7