(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 101877635 B
(45)授权公告日 2013.03.13

(21)申请号 201010159011.6

(22)申请日 2010.04.23

(30)优先权数据
2009-111578 2009.04.30 JP
2009-124035 2009.05.22 JP

(73)专利权人 索尼公司
地址 日本东京都

(72)发明人 作本纮一

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 康建峰 李春晖

(51)Int.Cl.
H04L 9/14(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 1439982 A,2003.09.03, 全文.
US 2008027865 A1,2008.01.31, 全文.

审查员 张博

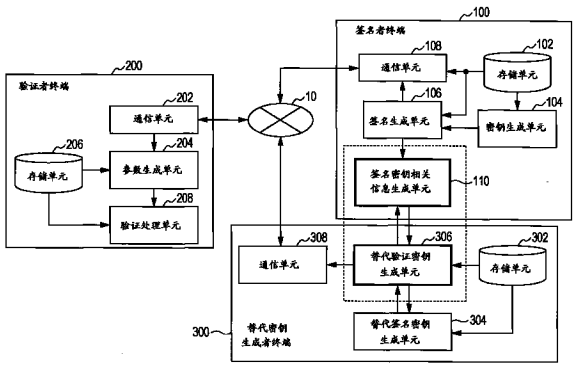
权利要求书 4 页 说明书 38 页 附图 24 页

(54)发明名称

图像处理装置及方法、电子签名生成系统及密钥生成方法

(57)摘要

本发明公开了一种图像处理装置、电子签名生成系统、电子签名密钥生成方法、图像处理方法、以及程序，其中所述图像处理装置包括：第一局部信息提供单元，用于将第一局部信息提供给持有与第一验证密钥KV相对应的第一签名密钥KS的其他设备，第一局部信息构成能够验证使用第一签名密钥KS生成的电子签名σ的第二验证密钥KV′的一部分并且不能确定第二验证密钥KV′，其中，所述第二验证密钥KV′与所述第一验证密钥KV不同；第二局部信息获取单元，用于获取其他设备使用第一局部信息和第一签名密钥KS生成的第二局部信息，第二局部信息不能确定第一签名密钥KS并且用于生成第二验证密钥KV′除第一局部信息之外的剩余部分；以及第二验证密钥生成单元，用于基于第一局部信息和第二局部信息生成第二验证密钥KV′。



CN 101877635 B

1. 一种图像处理装置，包括：

第一局部信息提供单元，用于将第一局部信息提供给持有与第一验证密钥 KV 相对应的第一签名密钥 KS 的其他设备，所述第一局部信息构成能够验证使用所述第一签名密钥 KS 生成的电子签名 σ 的第二验证密钥 KV′ 的一部分并且不能确定所述第二验证密钥 KV′，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同；

第二局部信息获取单元，用于获取其他设备使用所述第一局部信息和所述第一签名密钥 KS 生成的第二局部信息，所述第二局部信息不能确定所述第一签名密钥 KS 并且用于生成所述第二验证密钥 KV′ 除所述第一局部信息之外的剩余部分；以及

第二验证密钥生成单元，用于基于所述第一局部信息和所述第二局部信息生成所述第二验证密钥 KV′。

2. 根据权利要求 1 所述的图像处理装置，其中：

所述第一签名密钥 KS 被配置成包括 N1 个参数，其中，N1 ≥ 2；并且

所述第二局部信息获取单元获取使用利用所述第一局部信息以及所述第一签名密钥 KS 中所包括的 N1 个参数生成的参数而生成、并且不能确定所述第一签名密钥 KS 中所包括的各个参数的第二局部信息。

3. 根据权利要求 2 所述的图像处理装置，其中：

所述第二验证密钥 KV′ 被配置成包括 N2 个参数，其中，N2 ≥ 2；并且

所述第一局部信息提供单元提供所述第二验证密钥 KV′ 中所包括的 M2 个参数作为所述第一局部信息，其中，M2 ＜ N2。

4. 根据权利要求 2 所述的图像处理装置，其中：

所述第二验证密钥 KV′ 被配置成包括 N2 个参数，其中 N2 ≥ 2；并且

所述第一局部信息提供单元提供所述第二验证密钥 KV′ 中所包括的 M2 个参数以及除所述 M2 个参数之外的 N2-M2 个参数的散列值作为所述第一局部信息，其中 M2 ＜ N2。

5. 根据权利要求 1 所述的图像处理装置，其中：

如果在生成第二局部信息时对所述第一局部信息进行了基于所述其他设备所生成的随机数的预定运算处理，则所述第二局部信息获取单元获取所述其他设备所生成的随机数连同所述第二局部信息；并且

所述第二验证密钥生成单元基于所述第一局部信息、所述第二局部信息、以及所述随机数生成所述第二验证密钥 KV′。

6. 根据权利要求 1 所述的图像处理装置，其中：

所述其他设备是认证授权中心服务器；

所述图像处理装置还包括 ID 通知单元，用于将用以确定所述图像处理装置自身的 ID 信息通知给所述其他设备；并且

所述图像处理装置使用所述第一局部信息提供单元、所述第二局部信息获取单元和所述第二验证密钥生成单元，生成包括从所述 ID 通知单元接收到通知的其他设备所生成的 ID 信息的电子文件 m_{ID}，以及接受针对电子文件 m_{ID} 使用所述第一签名密钥 KS 生成的电子签名 σ_{ID} 的第二验证密钥 KV′；并且将所述电子文件 m_{ID} 和所述电子签名 σ_{ID} 用作用于证明所述第二验证密钥 KV′ 的有效性的电子证书。

7. 根据权利要求 1 所述的图像处理装置，其中：

所述装置自身是替代委托人的电子签名的代理所使用的代理终端；

所述其他设备是所述委托人使用的委托人终端；以及

所述图像处理装置使用第一局部信息提供单元、第二局部信息获取单元、以及第二验证密钥生成单元，生成至少包括所述委托人传递给代理的签名权限的内容的电子文件 m_w，以及接受针对所述电子文件 m_w 使用所述第一签名密钥 KS 而生成的电子签名 σ_w 的第二验证密钥 KV′；并且将所述电子文件 m_w 和所述电子签名 σ_w 用作用于证明所述第二验证密钥 KV′ 得到所述委托人承认的证书。

8. 一种图像处理装置，包括：

存储单元，存储成对的第一验证密钥 KV 和第一签名密钥 KS；

第一局部信息获取单元，获取构成能够验证使用所述第一签名密钥 KS 生成的电子签名 σ 的第二验证密钥 KV′ 的一部分并且不能确定所述第二验证密钥 KV′ 的第一局部信息，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同；

第二局部信息生成单元，使用所述第一签名密钥 KS 和所述第一局部信息获取单元所获取的第一局部信息生成第二局部信息，所述第二局部信息不能确定所述第一签名密钥 KS 并且用于生成所述第二验证密钥 KV′ 除所述第一局部信息之外的剩余部分；以及

第二局部信息提供单元，将所述第二局部信息生成单元所生成的第二局部信息提供给提供了所述第一局部信息的其他设备。

9. 根据权利要求 8 所述的图像处理装置，其中：

所述第一签名密钥 KS 被配置成包括 N1 个参数，其中，$N1 \geq 2$；并且

所述第二局部信息生成单元使用利用所述第一局部信息和所述第一签名密钥 KS 中所包括的 N1 个参数生成的参数生成第二局部信息，所述第二局部信息不能确定所述第一签名密钥 KS 中所包括的各个参数。

10. 根据权利要求 9 所述的图像处理装置，其中：

所述第二验证密钥 KV′ 被配置成包括 N2 个参数，其中，$N2 \geq 2$；并且

所述第一局部信息获取单元获取所述第二验证密钥 KV′ 中所包括的 M2 个参数作为所述第一局部信息，其中，$M2 < N2$。

11. 根据权利要求 9 所述的图像处理装置，其中：

所述第二验证密钥 KV′ 被配置成包括 N2 个参数，其中，$N2 \geq 2$；并且

所述第一局部信息获取单元获取所述第二验证密钥 KV′ 中所包括的 M2 个参数以及除所述 M2 个参数之外的 N2-M2 个参数的散列值作为所述第一局部信息，其中，$M2 < N2$。

12. 根据权利要求 8 所述的图像处理装置，还包括：

随机数生成器，生成随机数；以及

运算处理单元，使用所述随机数生成器所生成的随机数对所述第一局部信息进行预定运算处理，其中：

所述第二局部信息生成单元使用所述第一签名密钥 KS 和已经由所述运算处理单元进行了预定运算处理的第一局部信息生成所述第二局部信息；并且

所述第二局部信息提供单元将所述运算处理单元所使用的随机数连同所述第二局部信息一起提供给其他设备。

13. 一种电子签名生成系统，包括：

第一图像处理装置；以及

第二图像处理装置，其中：

所述第一图像处理装置包括：

存储单元，存储成对的第一验证密钥 KV 和第一签名密钥 KS；

第一局部信息获取单元，从所述第二图像处理装置获取构成能够验证使用所述第一签名密钥KS生成的电子签名 σ 的第二验证密钥KV′ 的一部分并且不能确定所述第二验证密钥 KV′ 的第一局部信息，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同；

第二局部信息生成单元，使用所述第一签名密钥 KS 和所述第一局部信息获取单元所获取的第一局部信息生成第二局部信息，所述第二局部信息不能确定所述第一签名密钥 KS 并且用于生成所述第二验证密钥 KV′ 除所述第一局部信息之外的剩余部分；以及

第二局部信息提供单元，将所述第二局部信息生成单元所生成的第二局部信息提供给提供了所述第一局部信息的所述第二图像处理装置；并且，

所述第二图像处理装置包括：

第一局部信息提供单元，将所述第一局部信息提供给所述第一图像处理装置；

第二局部信息获取单元，获取所述第二局部信息；以及

第二验证密钥生成单元，基于所述第一局部信息和所述第二局部信息生成所述第二验证密钥 KV′。

14. 一种电子签名密钥生成方法，包括：

第一局部信息提供步骤，用于将第一局部信息提供给持有与第一验证密钥 KV 相对应的第一签名密钥 KS 的其他设备，所述第一局部信息构成能够验证使用所述第一签名密钥 KS 生成的电子签名 σ 的第二验证密钥 KV′ 的一部分并且不能确定所述第二验证密钥 KV′，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同；

第二局部信息获取步骤，用于获取其他设备使用所述第一局部信息和所述第一签名密钥 KS 生成的第二局部信息，所述第二局部信息不能确定所述第一签名密钥 KS 并且用于生成所述第二验证密钥 KV′ 除所述第一局部信息之外的剩余部分；以及

第二验证密钥生成步骤，用于基于所述第一局部信息和所述第二局部信息生成所述第二验证密钥 KV′。

15. 一种图像处理方法，包括：

第一局部信息获取步骤，用于获取构成能够验证使用与第一验证密钥 KV 成对的第一签名密钥KS生成的电子签名 σ 的第二验证密钥KV′ 的一部分并且不能确定所述第二验证密钥 KV′ 的第一局部信息，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同；

第二局部信息生成步骤，用于使用所述第一签名密钥 KS 和所述第一局部信息获取步骤中所获取的第一局部信息生成第二局部信息，所述第二局部信息不能确定所述第一签名密钥 KS 并且用于生成所述第二验证密钥 KV′ 除所述第一局部信息之外的剩余部分；以及

第二局部信息提供步骤，用于将第二局部信息生成步骤中所生成的所述第二局部信息提供给提供了所述第一局部信息的其他设备。

16. 一种电子签名密钥生成方法，包括：

第一局部信息提供步骤，其中第二图像处理装置将第一局部信息提供给第一图像处理装置，所述第一局部信息构成能够验证使用与第一验证密钥 KV 成对的第一签名密钥 KS 生

成的电子签名 σ 的第二验证密钥 KV′ 的一部分并且不能确定所述第二验证密钥 KV′，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同；

第一局部信息获取步骤，其中第一图像处理装置从所述第二图像处理装置获取所述第一局部信息；

第二局部信息生成步骤，其中所述第一图像处理装置使用所述第一签名密钥 KS 和所述第一局部信息获取步骤中所获取的第一局部信息生成第二局部信息，所述第二局部信息不能确定所述第一签名密钥 KS 并且用于生成所述第二验证密钥 KV′ 除所述第一局部信息之外的剩余部分；

第二局部信息提供步骤，其中所述第一图像处理装置将所述第二局部信息生成步骤中所生成的第二局部信息提供给提供了所述第一局部信息的所述第二图像处理装置；

第二局部信息获取步骤，其中所述第二图像处理装置获取所述第二局部信息；以及

第二验证密钥生成步骤，其中所述第二图像处理装置基于所述第一局部信息和所述第二局部信息生成所述第二验证密钥 KV′。

图像处理装置及方法、电子签名生成系统及密钥生成方法

技术领域

[0001] 本发明涉及图像处理装置、电子签名生成系统、电子签名密钥生成方法、图像处理方法、以及程序。

背景技术

[0002] 通常，为了证明文件作者身份，作者在该文件上放置签名、印章等（在下文中称作签名）。此签名表明署名的人对该文件中描述的内容负责。如果文件是纸质文件，则文件的作者添加他们的手写签名。另一方面，如果文件是电子文件，则签名者难以将印章印在电子数据上或者在其上放置他 / 她的亲笔签名。为此，使用了一种附加被称为电子签名的数据以通过这些电子签名唯一地识别签名者的方法。近年来，各种文件被数字化从而电子签名的重要性日益增加。在这种情况下，存在许多情形，其中防止电子签名伪造成为一个问题。虽然附加到纸质文件上的签名具有同样的问题，但是对电子签名需要更多的关注，因为电子数据更容易复制。

[0003] 电子签名方案的公知示例是 ElGamal 签名方案。此方案基于离散对数问题的困难性。首先，签名者生成用于生成电子签名的签名密钥以及用于验证电子签名有效性的验证密钥。此外，签名者将验证密钥公开。随后，签名者生成电子文件并使用签名密钥生成电子签名，将电子签名连同电子文件一起提供给验证者。为此，验证者能够使用公开的验证密钥来验证电子签名。在 ElGamal 签名方案的情形中，当某人试图根据验证密钥生成签名密钥或电子签名时，需要解决离散对数问题，离散对数问题是难以解决的，因为它涉及大量运算。根据电子签名生成签名密钥存在同样的困难性。这种困难性防止了签名伪造。

[0004] 然而，如果签名密钥由于某些原因泄漏给第三方，则第三方可以随意地伪造电子签名。因此，当签名密钥泄漏时，难以区分用签名密钥生成的电子签名是属于真正的签名者还是它是由第三方伪造的。在签名被附加到纸质文件上的情形中，可以相对容易地区分复制品和原件。然而，在电子数据的情形中，难以正确地对它们进行区分。为此，采用了一种对策以在 发现签名密钥泄漏的任何阶段使电子签名、签名密钥、以及验证密钥无效。此时，也使得其上附加有电子签名的电子文件基本上无效。

[0005] 已经提出了各种方案以减少与签名密钥泄漏相关联的问题。例如，第 3640785 号日本专利描述了一种方法，该方法针对每个时段设置不同的签名密钥，以使得各个签名密钥只针对相应时段内生成的电子签名有效（见图 21）。根据此方法，当签名密钥泄漏并因此该签名密钥被弃用时，仍然可以维持早于或晚于该签名密钥所对应的时段的时段的签名密钥有效。为此，不必使泄漏的签名密钥所对应的时段以及其上附加有该签名密钥的电子文件以外的、其它时段内生成的电子签名无效。结果，可以减少被无效的电子文件的数量。

发明内容

[0006] 然而，即使在使用第 3640785 号日本专利中所描述的技术的情况下，泄漏的签名密钥所对应的时段中生成的所有电子签名将会无效，并且基本上其上附加有该签名密钥的

所有电子文件将会无效。当然，即使签名密钥没有泄漏，但是如果发生使该签名密钥无效的原因，则将会存在以同样地方式被变为无效的电子文件。如上所述，电子签名的作用与附加到纸质文件上的签名的作用是一样的。因此，取决于电子文件的种类，存在不容易将电子签名再次附加到电子文件上的情形。

[0007] 为此，严格管理签名密钥以使其不被泄漏从而不使电子签名无效是极其重要的。然而，难以保证签名密钥永远不泄漏。此处，即使在用于生成某个电子签名的签名密钥泄漏的情况下，如果可以产生针对该电子签名（以及相应的电子文件）有效的另一验证密钥，则该电子签名将不会无效。另外，为这种原因以外的目的起见，可能存在如下情形：便于拥有一种算法，能够安全地生成对于某个电子签名和相应的电子文件有效的多个验证密钥。

[0008] 关于上述算法，已知有 Sakumoto 和 Tanaka 的如下研究报告（下文中称作 SC08 方案）。SC08 方案：Koichi Sakumotoand Keisuke Tanaka, ″ Key-Substitutable Signature ″, The 2008 Symposium on Cryptography and Information Security, Miyazaki, Japan, Jan. 22-25, 2008。

[0009] SC08 方案是允许实体（在下文中称作替代签名者）能够与签名者交互以生成对于某个电子签名和相应的电子文件有效的验证密钥（在下文中 称作替代验证密钥）。在 SC08 方案中，通过提供一种在与签名者的交互过程中生成替代验证密钥的算法（在下文中称作交互式算法），防止了除替代签名者以外的第三方能够随意地生成替代验证密钥。然而，在 SC08 方案中，由于签名者基本上按交互式算法生成替代验证密钥，因此对于替代签名者使用替代验证密钥所对应的签名密钥生成的电子签名的安全性存在一些担心。

[0010] 因此，期望提供新的或改进的图像处理装置、电子签名生成系统、电子签名密钥生成方法、图像处理方法、以及程序，能够更安全地使用交互式算法生成替代验证密钥。

[0011] 根据本发明的一个实施例，提供了一种图像处理装置，包括：第一局部信息提供单元，用于将第一局部信息提供给持有第一验证密钥 KV 所对应的第一签名密钥 KS 的其他设备，第一局部信息构成能够验证使用第一签名密钥 KS 生成的电子签名 σ 的第二验证密钥 KV′ 的一部分并且不能确定第二验证密钥 KV′，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同；第二局部信息获取单元，用于获取其他设备使用第一局部信息和第一签名密钥 KS 生成的第二局部信息，第二局部信息不能确定第一签名密钥 KS 并且用于生成第二验证密钥 KV′ 除第一局部信息之外的剩余部分；以及第二验证密钥生成单元，用于基于第一局部信息和第二局部信息生成第二验证密钥 KV′。

[0012] 第一签名密钥 KS 可以被配置成包括 N1 个参数，其中，$N1 \geq 2$；并且第二局部信息获取单元可以被配置成获取使用利用第一局部信息以及第一签名密钥 KS 中所包括的 N1 个参数生成的参数所生成的并且不能确定第一签名密钥 KS 中所包括的各个参数的第二局部信息。

[0013] 第二验证密钥 KV′ 可以被配置成包括 N2 个参数，其中，$N2 \geq 2$；并且第一局部信息提供单元可以被配置成提供第二验证密钥 KV′ 中所包括的 M2 个参数作为第一局部信息，其中，$M2 < N2$。

[0014] 第二验证密钥 KV′ 可以被配置成包括 N2 个参数，其中，$N2 \geq 2$；并且第一局部信息提供单元可以被配置成提供第二验证密钥 KV′ 中所包括的 M2 个参数以及除 M2 个参数之外的 N2-M2 个参数的散列值作为第一局部信息，其中，$M2 < N2$。

[0015] 如果在生成第二局部信息时已经对第一局部信息进行了基于其他设备所生成的随机数的预定运算处理，则第二局部信息获取单元可以被配置 成获取其他设备所生成的随机数连同第二局部信息。在此情形中，第二验证密钥生成单元基于第一局部信息、第二局部信息、以及随机数生成第二验证密钥 KV′ 。

[0016] 根据本发明的另一个实施例，提供了一种图像处理装置，包括 ：存储单元，用于存储成对的第一验证密钥 KV 和第一签名密钥 KS ；第一局部信息获取单元，用于获取构成能够验证使用第一签名密钥 KS 生成的电子签名 σ 的第二验证密钥 KV′ 的一部分并且不能确定第二验证密钥 KV′ 的第一局部信息，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同 ；第二局部信息生成单元，用于使用第一签名密钥 KS 以及第一局部信息获取单元所获取的第一局部信息生成第二局部信息，第二局部信息不能确定第一签名密钥 KS 并且用于生成第二验证密钥 KV′ 除第一局部信息之外的剩余部分 ；以及第二局部信息提供单元，用于将第二局部信息生成单元所生成的第二局部信息提供给提供了第一局部信息的其他设备。

[0017] 第一签名密钥 KS 可以被配置成包括 N1 个参数，其中，N1 ≥ 2 ；并且第二局部信息生成单元可以被配置成使用利用第一局部信息以及第一签名密钥 KS 中所包括的 N1 个参数生成的参数生成第二局部信息，第二局部信息不能确定第一签名密钥 KS 中所包括的各个参数。

[0018] 第二验证密钥 KV′ 可以被配置成包括 N2 个参数，其中，N2 ≥ 2 ；并且第一局部信息获取单元可以被配置成获取第二验证密钥 KV′ 中所包括的 M2 个参数作为第一局部信息，其中，M2 ＜ N2。

[0019] 第二验证密钥 KV′ 可以被配置成包括 N2 个参数，其中，N2 ≥ 2 ；并且第一局部信息获取单元可以被配置成获取第二验证密钥 KV′ 中所包括的 M2 个参数以及除 M2 个参数之外的 N2-M2 个参数的散列值作为第一局部信息，其中，M2 ＜ N2。

[0020] 该图像处理装置还可以包括 ：随机数生成器，用于生成随机数 ；以及运算处理单元，用于使用随机数生成器所生成的随机数对第一局部信息进行预定运算处理。在此情形中，第二局部信息生成单元可以被配置成使用第一签名密钥 KS 以及已经由运算处理单元进行了预定运算处理的第一局部信息生成第二局部信息 ；并且第二局部信息提供单元可以被配置成将运算处理单元所使用的随机数连同第二局部信息一起提供给其他设备。

[0021] 根据本发明的另一个实施例，提供了一种电子签名生成系统，包括 ：第一图像处理装置 ；第二图像处理装置，其中 ：第一图像处理装置包括 ： 存储单元，用于存储成对的第一验证密钥 KV 和第一签名密钥 KS ；第一局部信息获取单元，用于从第二图像处理装置获取构成能够验证使用第一签名密钥 KS 生成的电子签名 σ 的第二验证密钥 KV′ 的一部分并且不能确定第二验证密钥 KV′ 的第一局部信息，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同 ；第二局部信息生成单元，用于使用第一签名密钥 KS 以及第一局部信息获取单元所获取的第一局部信息生成第二局部信息，第二局部信息不能确定第一签名密钥 KS 并用于生成第二验证密钥 KV′ 除第一局部信息之外的剩余部分 ；以及第二局部信息提供单元，用于将第二局部信息生成单元所生成的第二局部信息提供给提供了第一局部信息的第二图像处理装置 ；并且，第二图像处理装置包括 ：第一局部信息提供单元，用于将第一局部信息提供给第一图像处理装置 ；第二局部信息获取单元，用于获取第二局部信息 ；以及

第二验证密钥生成单元，用于基于第一局部信息和第二局部信息生成第二验证密钥 KV′ 。

[0022] 根据本发明的另一个实施例，提供了一种电子签名密钥生成方法，包括：第一局部信息提供步骤，用于将第一局部信息提供给持有第一验证密钥 KV 所对应的第一签名密钥 KS 的其他设备，第一局部信息构成能够验证使用第一签名密钥 KS 生成的电子签名 σ 的第二验证密钥 KV′ 的一部分并且不能确定第二验证密钥 KV′ ，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同；第二局部信息获取步骤，用于获取其他设备使用第一局部信息和第一签名密钥 KS 生成的第二局部信息，第二局部信息不能确定第一签名密钥 KS 并且用于生成第二验证密钥 KV′ 除第一局部信息之外的剩余部分；以及第二验证密钥生成步骤，用于基于第一局部信息和第二局部信息生成第二验证密钥 KV′ 。

[0023] 根据本发明的另一个实施例，提供了一种图像处理方法，包括：第一局部信息获取步骤，用于获取构成能够验证使用与第一验证密钥 KV 成对的第一签名密钥 KS 生成的电子签名 σ 验证的第二验证密钥 KV′ 的一部分并且不能确定第二验证密钥 KV′ 的第一局部信息，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同；第二局部信息生成步骤，用于使用第一签名密钥 KS 以及在第一局部信息获取步骤中所获取的第一局部信息生成第二局部信息，第二局部信息不能确定第一签名密钥 KS 并且用于生成第二验证密钥 KV′ 除第一局部信息之外的剩余部分；以及第二局部信息提供步骤，用于将第二局部信息生成步骤中所生成的第二局部信息提供给提供了第一局部信息的其他设备。

[0024] 根据本发明的另一个实施例，提供了一种电子签名密钥生成方法，包括：第一局部信息获取步骤，其中第二图像处理装置提供构成能够使用与第一验证密钥 KV 成对的第一签名密钥 KS 生成的电子签名 σ 的第二验证密钥 KV′ 的一部分并且不能确定第二验证密钥 KV′ 的第一局部信息，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同；第一局部信息获取步骤，其中第一图像处理装置从第二图像处理装置获取第一局部信息；第二局部信息生成步骤，其中第一图像处理装置使用第一签名密钥 KS 以及第一局部信息获取步骤中所获取的第一局部信息生成第二局部信息，第二局部信息不能确定第一签名密钥 KS 并且用于生成第二验证密钥 KV′ 除第一局部信息之外的剩余部分；第二局部信息提供步骤，其中第一图像处理装置将第二局部信息生成步骤中所生成的第二局部信息提供给提供了第一局部信息的第二图像处理装置；第二局部信息获取步骤，其中第二图像处理装置获取第二局部信息；以及第二验证密钥生成步骤，其中第二图像处理装置基于第一局部信息和第二局部信息生成第二验证密钥 KV′ 。

[0025] 根据本发明的另一个实施例，提供了一种用于使计算机实现如下功能的程序：第一局部信息提供功能，用于将第一局部信息提供给持有第一验证密钥 KV 所对应的第一签名密钥 KS 的其他设备，第一局部信息构成能够验证使用第一签名密钥 KS 生成的电子签名 σ 的第二验证密钥 KV′ 的一部分并且不能确定第二验证密钥 KV′ ，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同；第二局部信息获取功能，用于获取其他设备使用第一局部信息和第一签名密钥 KS 生成的第二局部信息，第二局部信息不能确定第一签名密钥 KS 并且用于生成第二验证密钥 KV′ 除第一局部信息之外的剩余部分；以及第二验证密钥生成功能，用于基于第一局部信息和第二局部信息生成第二验证密钥 KV′ 。

[0026] 根据本发明的另一个实施例，提供了一种用于使计算机实现如下功能的程序：第一局部信息获取功能，用于获取构成能够验证使用与第一验证密钥 KV 成对的第一签名密

钥 KS 生成的电子签名 σ 的第二验证密钥 KV′ 的一部分并且不能确定第二验证密钥 KV′ 的第一局部信息，其中，所述第二验证密钥 KV′ 与所述第一验证密钥 KV 不同；第二局部信息生成功能，用于使用第一签名密钥 KS 以及通过第一局部信息获取功能所获取的第一局部信息生成第二局部信息，第二局部信息不能确定第一签名密钥 KS 并且用于生成第二验证密钥 KV′ 除第一局部信息之外的剩余部分；以及第二局部信息提供功能，用于将通过第二局部信息生成功能生成的第二局部信 息提供给提供了第一局部信息的其他设备。

[0027] 在该图像处理装置中，其他设备可以是认证授权中心服务器。此外，图像处理装置还可以包括：ID 通知单元，用于将用以识别装置自身的 ID 信息通知给其他设备。另外，图像处理装置可以被配置成生成包括从 ID 通知单元接收到通知的其他设备所生成的 ID 信息的电子文件 m_{ID}，以及接受针对电子文件 m_{ID} 使用第一签名密钥 KS 生成的电子签名 σ_{ID} 的第二验证密钥 KV′；并将电子文件 m_{ID} 和电子签名 σ_{ID} 用作用于证明第二验证密钥 KV′ 的有效性的电子证书。

[0028] 在该图像处理装置中，第一设备可以是替代委托人的电子签名的代理所使用的代理终端。此外，其他设备可以是委托人所使用的委托人终端。此外，图像处理装置可以被配置成使用第一局部信息提供单元、第二局部信息获取单元、以及第二验证密钥生成单元生成至少包括委托人传递给代理的签名权限的内容的电子文件 m_w，以及接受针对电子文件 m_w 使用第一签名密钥 KS 生成的电子签名 σ_w 的第二验证密钥 KV′；并将电子文件 m_w 和电子签名 σ_w 用作用于证明第二验证密钥 KV′ 得到委托人承认的证书。

[0029] 根据本发明的另一个实施例，可以提供一种能够在计算机中实现电子签名生成系统的功能的程序。根据本发明的另一个实施例，可以提供一种记录程序的计算机可读记录介质。

[0030] 如上所述，根据本发明的实施例，可以使用交互式算法更安全地生成替代验证密钥。

附图说明

[0031] 图 1 是示意性地示出了当用于生成电子签名的签名密钥泄漏时出现的问题的图；

[0032] 图 2 是示出了作为密钥可替代电子签名方案的示例的 SC08 方案的实体的一个示范性配置的图；

[0033] 图 3 是示出了根据 SC08 方案的替代密钥生成方法、电子签名生成方法、以及电子签名验证方法的图；

[0034] 图 4 是示出了替代验证密钥的属性的图；

[0035] 图 5 是示出了根据 SC08 方案的替代密钥生成方法的流程的图；

[0036] 图 6 是示出了根据 SC08 方案的系统参数生成方法的图；

[0037] 图 7 是示出了根据 SC08 方案的电子签名生成方法的图；

[0038] 图 8 是示出了根据 SC08 方案的电子签名验证方法的图；

[0039] 图 9 是详细示出了根据 SC08 方案的替代密钥生成方法的图；

[0040] 图 10 是示出了根据本发明的第一实施例的替代密钥生成方法的流程的图；

[0041] 图 11 是示出了根据第一实施例的电子签名生成方法的图；

[0042] 图 12 是示出了根据第一实施例的电子签名验证方法的图；

[0043] 图 13 是详细示出了根据第一实施例的替代密钥生成方法的图；

[0044] 图 14 是示出了根据第一实施例的密钥更新系统的一个示范性配置以及签名者终端、验证者终端和替代密钥生成者终端的示范性功能配置的图；

[0045] 图 15 是示出了根据本发明的第二实施例的电子签名生成方法的图；

[0046] 图 16 是示出了根据第二实施例的电子签名验证方法的图；

[0047] 图 17 是详细示出了根据第二实施例的替代密钥生成方法的图；

[0048] 图 18 是示出了根据本发明的第一和第二实施例的一种修改的替代密钥生成方法的流程的图；

[0049] 图 19 是示出了根据本发明的第一和第二实施例的签名者终端和验证者终端的示范性硬件配置的图；

[0050] 图 20 是示意性地示出了根据带期限的电子签名方案的密钥更新方法的图；

[0051] 图 21 是示出了在根据本发明的第一和第二实施例的替代密钥生成方法应用于 PKI 认证授权中心服务器与用户终端之间的密钥认证情况下的示范性系统配置的图；

[0052] 图 22 是示出了在根据本发明的第一和第二实施例的替代密钥生成方法应用于 PKI 认证授权中心服务器与用户终端之间的密钥认证情况下的应用方法的图；

[0053] 图 23 是示出了在根据本发明的第一和第二实施例的替代密钥生成方法应用于代理签名方案的代理认证情况下的示范性系统配置的图；以及

[0054] 图 24 是示出了在根据本发明的第一和第二实施例的替代密钥生成方法应用于代理签名方案的代理认证情况下的应用方法的图。

具体实施方式

[0055] 在下文中，将参照附图描述本发明的优选实施例。在整个说明书和附图中，具有基本上相同的功能配置的组成元件将用相同的参考标号表示，并将省略对其的重复描述。

[0056] 描述流程

[0057] 此处，将简要提及对下述本发明的实施例的描述流程。首先，通过参照图 1，将简要描述在用于电子签名方案中的签名密钥泄漏时出现的问题。另外，通过参照图 21，将简要描述针对签名密钥泄漏的典型对策，并对其问题进行讨论。

[0058] 随后，通过参照图 2 和图 3，将对 SC08 方案和根据本实施例的密钥可替代电子签名方案的实体的配置以及每个实体所执行的过程进行描述。此后，通过参照图 4，将对根据本实施例的密钥更新方法中所使用的替代密钥的属性以及替代密钥的要求进行描述。然后，通过参照图 5 至图 9，将对 SC08 方案的替代密钥生成方法进行详细描述。在此部分中，将对 SC08 方案的问题进行讨论。

[0059] 随后，通过参照图 10 至图 14，将对根据本发明的第一实施例的密钥可替代电子签名方案（下文中称作本方案 1）以及密钥更新系统的配置进行详细描述。在此部分中，还将对根据该实施例的密钥可替代电子签名方案的具体算法进行详细描述。另外，还将对根据该实施例的密钥更新系统的系统配置以及签名者终端、验证者终端、和替代密钥生成者终端的功能配置进行描述。

[0060] 然后，通过参照图 15 至图 17，将对根据本发明的第二实施例的密钥可替代电子签名方案（下文中称作本方案 2）以及密钥更新系统的配置进行详细描述。在此部分中，还将

对根据该实施例的密钥可替代电子签名方案的具体算法进行详细描述。然而，将不再对根据该实施例的密钥更新系统的系统配置以及签名者终端、验证者终端、和替代密钥生成者终端的功能配置进行描述，因为它们基本上与第一实施例的相同。

[0061] 然后，通过参照图 18，将对根据本发明的第一和第二实施例的替代密钥生成方法的一种修改进行描述。此后，通过参照图 20，将对根据该 实施例的签名者终端和验证者终端的示范性硬件配置进行描述。然后，通过参照图 21 和图 22，将对根据第一和第二实施例的替代密钥生成方法应用于 PKI 的应用方法进行描述。此后，通过参照图 23 和图 24，将对根据第一和第二实施例的替代密钥生成方法应用于代理签名方案的应用方法进行描述。然后，将对根据第一和第二实施例的替代密钥生成方法应用于角色共享电子签名方案的应用方法进行描述。

[0062] 描述项

[0063] 1 :引言

[0064] 1-1 :签名密钥的泄漏

[0065] 1-2 :带期限的签名方案

[0066] 1-3 :系统配置

[0067] 1-4 :替代验证密钥的属性

[0068] 1-5 :SC08 方案的替代密钥生成方法

[0069] 1-6 :SC08 方案的算法

[0070] 2 :第一实施例

[0071] 2-1 :替代密钥生成方法

[0072] 2-2 :算法

[0073] 2-3 :终端的功能配置

[0074] 3 :第二实施例

[0075] 3-1 :算法

[0076] 4 :对第一和第二实施例的修改

[0077] 4-1 :替代密钥生成方法

[0078] 5 :终端的示范性硬件配置

[0079] 6 :应用示例

[0080] 6-1 :应用于 PKI

[0081] 6-2 :应用于代理签名方案

[0082] 6-3 :应用于角色共享电子签名

[0083] 1 :引言

[0084] 首先，在详细描述本发明的实施例以前，为了帮助更好地理解实施例的技术要点以及技术内容，将简要描述为了理解所应该参照的技术内容的细节。在此部分中，将对被认为是实施例的技术的开发基础的 SC08 方案的替代密钥生成方法及其算法进行描述。

[0085] 1-1 :签名密钥的泄漏

[0086] 首先，将通过参照图 1 简要描述签名密钥的泄漏。在图 1 中，示意性地示出了当用于生成附加到电子文件 m 上的电子签名 σ 的签名密钥 sk 被泄漏时所出现的问题。

[0087] 如图 1 中所示，使用与签名密钥 sk 成对的有效验证密钥 pk 可以对使用签名密钥

sk 附加到电子文件 m 上的有效电子签名 σ 进行验证。公开验证密钥 pk。此外，在此验证中，使用预定的验证公式。即，验证者输入电子文件 m、电子签名 σ、以及关于针对预定验证公式的验证密钥 pk 的信息并且确定预定验证公式是否有效，从而验证电子签名 σ 的有效性。以此方式，当针对验证密钥 pk 确定电子文件 m 的电子签名 σ 有效时，判定“验证密钥 pk 接受电子签名 σ 和电子文件 m 对 (m，σ)”。

[0088] 然而，签名密钥 sk 由签名者秘密管理并且通常不会被其他人获知。当然，签名者将会管理签名密钥 sk 以不被验证者获知。然而，难以保证签名密钥 sk 永远不泄漏。例如，存在许多情形，其中签名者所使用的终端被攻击，终端中所存储的关于签名密钥 sk 的信息泄漏出去。同样，当签名密钥 sk 由于某些原因泄漏给对手（下文中称作攻击者）时 (S1)，攻击者能够将电子签名 σ 附加到任何电子文件上。也就是说，电子签名 σ 被伪造。

[0089] 例如，让我们考虑攻击者使用泄漏的签名密钥 sk 将电子签名 σ 附加到电子文件 m1 上的情形。在此情形中，由于附加到电子文件 m1 上的电子签名 σ 是使用有效签名密钥 sk 生成的，电子签名 σ 将会被验证密钥 pk 接受。即，虽然签名是由攻击者生成的，但是它被作为有效签名者的签名接受。例如，如果电子文件 m1 是房地产购买合同，则有效签名者面临他 / 她自己的房地产在签名者不知情的情况下被随意卖出的危险。

[0090] 因此，有效签名者将会在觉察到签名密钥 sk 泄漏时使签名密钥 sk 无效 (S2)。当签名密钥 sk 被无效时，与签名密钥 sk 成对的验证密钥 pk 也被无效。另外，用签名密钥 sk 生成的电子签名 σ 也被无效。例如，如果电子文件 m 是合同，则当电子签名 σ 被无效时，使用该电子文件交易 的合同将会被无效。如果电子文件 m 是重要性低的内部办公文件，则可以使用新生成的签名密钥 sk′ 附加另一个电子签名 σ′ 。然而，在许多情形中，如果电子文件 m 是诸如与第三方交易的合同等的重要文件，则难以只是简单地再次放入签名。

[0091] 如果管理许多这种重要文件，则泄漏签名密钥 sk 的问题是严重的。已经考虑了各种对策以解决过去生成的电子签名 σ 随签名密钥 sk 的泄漏也被无效的问题。然而，这些对策中的大多数对策只能够减少随签名密钥 sk 的泄漏被无效的电子签名 σ 的影响，但它们不是用于恢复已经被无效的电子签名 σ 的方法。此处，将带期限的签名方案作为针对签名密钥 sk 泄漏的对策的示例进行介绍。

[0092] 1-2 :带期限的签名方案

[0093] 带期限的签名方案是如图 20 中所示的方案。在此方案中，每隔预定时段对签名密钥 sk 进行更新。另一方面，假定贯穿全部时段使用相同的验证密钥 pk。例如，在时段 1 中使用签名密钥 sk1，并生成仅在时段 1 内有效的电子签名。当时间过去并进入时段 2 时，使用仅在时段 2 内有效的签名密钥 sk2，并生成仅在时段 2 内有效的电子签名。在此方案中，即使使用签名密钥 sk1 在时段 2 内生成电子签名，该电子签名也不被验证密钥 pk 接受。

[0094] 因此，即使如图 20 中步骤 B 所示在签名密钥 sk1、sk3、以及 sk4 被泄漏且如步骤 C 所示在时段 1、3、4 内生成的电子签名被无效时，时段 2、5、.....、等内生成的电子签名仍然会保持为有效。为此，不必使其上附加有使用签名密钥 sk2、sk5、.....、等在时段 2、5、.....、等内生成的电子签名的电子文件无效。然而，此方案没有达到对上述问题的根本解决，因为其上附加有在时段 1、3、以及 4 内生成的电子签名的电子文件被无效。毕竟，对上述问题的解决方案需要用于恢复用泄漏前的签名密钥 sk 生成的电子签名 σ 的方法。

[0095] 鉴于这些原因，本发明人构思了如下思想 :生成其他验证密钥 pk′ ，该验证密钥

pk′ 不接受攻击者伪造的电子签名 σ 而只接受过去有效签名者附加到电子文件 m 上的电子签名 σ。然而，生成这种其他验证密钥 pk′ 的同时确保足够的安全性是不容易的。但是，在使用 SC08 方案中所称的替代密钥时可以获得这种其他验证密钥 pk′。因此，本发明人注意到 SC08 方案。

[0096] 后面所描述的 SC08 方案并非仅被开发用于上述目的，而是被开发意在使得能够生成针对任何电子签名和电子文件对都是安全的多个验证密钥。即，SC08 方案并非开发用于有限的应用。因此，应当注意，SC08 方案可以用于各种应用。此外，应当注意，虽然后面所描述的实施例的技术向 SC08 方案引入了额外的想法，但是这些技术也可以应用于宽范围的应用。

[0097] 1-3：系统配置

[0098] 此处，将对根据 SC08 方案以及后面所描述的实施例中使用的方案的电子签名系统的模型进行描述。在这些方案中，电子签名系统的模型由五个实体指定。如图 2 中所示，五个实体是系统管理员、签名者、验证者、认证授权中心、以及替代签名者（在下文中称作替代密钥生成者）。

[0099] 系统管理员是使用系统参数生成算法 (SetupKSS) 生成系统参数 cp 的实体。签名者是使用密钥生成算法 (GenKSS) 生成对各个签名者唯一的签名密钥 sk 以及与签名密钥 sk 成对的验证密钥 pk 的实体。此外，签名者使用签名生成算法 (SigKSS) 生成电子文件 m 的电子签名 σ。

[0100] 验证者是使用签名验证算法 (Ver) 对附加到电子文件 m 上的电子签名 σ 的有效性进行验证的实体。替代密钥生成者是使用替代密钥生成算法 <ORG(sk),SUB> 生成替代签名密钥 sk′ 以及与替代签名密钥 sk′ 成对的替代验证密钥 pk′ 的实体。然而，在生成某个电子文件 m 的替代密钥以及附加到该电子文件 m 上的电子签名 σ 时，替代密钥生成者生成替代密钥的同时执行与签名者的交互，其中签名者是附加到该电子文件 m 上的电子签名 σ 的生成者。此外，认证授权中心是发布用于保证验证密钥或者签名者或替代密钥生成者所生成的替代验证密钥的有效性的证书的实体。

[0101] 这些实体执行如图 3 中所示的过程，从而实现签名密钥 sk 和验证密钥 pk 的生成、电子签名 σ 的生成、替代签名密钥 sk′ 和替代验证密钥 pk′ 的生成、以及电子签名 σ 的验证。假设系统参数 cp 已经由系统管理员使用系统参数生成算法 (SetupKSS) 生成。使用 SetupKSS 生成 cp 如下面的公式 1 所示。在该公式中，1^{λ} 是安全性参数。

[0102] $cp = SetupKSS(1^{\lambda})...(1)$

[0103] 签名者的密钥生成步骤

[0104] 首先，将对签名者所执行的密钥生成过程进行描述。如图 3 中所示，签名者在密钥生成步骤中从系统管理员获取系统参数 cp。然后，签名者 将系统参数 cp 输入到密钥生成算法 (GenKSS) 中以生成签名密钥 sk 和验证密钥 pk 对。使用 GenKSS 生成 (sk,pk) 如下面公式 (2) 所示。在使用密钥生成算法 GenKSS 生成签名密钥 sk 和验证密钥 pk 时，签名者将所生成的签名密钥 sk 和验证密钥 pk 以成对的方式存储。此外，如果有必要，则签名者将验证密钥 pk 作为它自身的验证密钥向认证授权中心注册并接收其证书。

[0105] $(sk,pk) = GenKSS(cp)...(2)$

[0106] 签名者的签名生成步骤

[0107] 接下来，将描述签名者所执行的签名生成过程。如图 3 中所示，签名者准备其上将会附加有签名的电子文件 m 以及签名者中所存储的签名密钥 sk。然后，签名者将签名密钥 sk 和电子文件 m 输入到签名生成算法 (SigKSS) 中以生成电子签名 σ。使用 SigKSS 生成 σ 如下面公式 (3) 所示。然后，签名者将通过下面的公式 (3) 生成的电子签名 σ（算法的输出）设置为电子文件 m 的电子签名 σ。

[0108] $\sigma = SigKSS(sk, m)$...(3)

[0109] 签名者和替代签名者的替代密钥生成步骤

[0110] 接下来，将对签名者和替代签名者合作执行的替代密钥生成过程的概况进行描述。替代密钥生成方法的细节将在后面进行描述。首先，签名者准备电子文件 m、电子签名 σ、用于生成电子签名 σ 的签名密钥 sk 以及与签名密钥 sk 成对的验证密钥 pk。然后，签名者将所准备的电子文件 m、电子签名 σ、以及验证密钥 pk 提供给替代密钥生成者。此时，替代密钥生成者从签名者获取电子文件 m、电子签名 σ、以及验证密钥 pk。

[0111] 然后，签名者和替代密钥生成者将验证密钥 pk、电子文件 m、以及电子签名 σ 作为公共参数输入给替代密钥生成算法 <ORG(sk), SUB>。另外，签名者在与替代密钥生成者交互的过程中生成接受电子文件 m 和电子签名 σ 的替代验证密钥 pk′ 以及与替代验证密钥 pk′ 成对的替代签名密钥 sk′。如后面所描述的，应当注意，虽然在 SC08 方案中，“实际上，签名者生成替代密钥”，但是在后面所描述的实施例的方案中，“替代密钥生成者生成替代密钥”。这是决定两个方案之间在安全性方面的不同的最大的区别。

[0112] 此外，使用 <ORG(sk), SUB> 生成 sk′ 和 pk′ 如下面的公式 (4) 所示。此处，ORG 对应于签名者，SUB 对应于替代密钥生成者。即，ORG (sk) 表明签名者在替代密钥生成算法中使用签名密钥 sk。然而，签名密钥 sk 不呈现给替代密钥生成者 SUB，而是用于终止于签名者 ORG 一侧的运算，只将其运算结果提供给替代密钥生成者。其细节将在后面进行描述。在通过下面的公式 4 生成替代签名密钥 sk′ 和替代验证密钥 pk′ 时，如果有必要，则替代密钥生成者将替代验证密钥 pk′ 作为它自身的验证密钥向认证授权中心注册，并接收其证书。

[0113] $(sk', pk') = \langle ORG(sk), SUB\rangle(pk, m, \sigma)$...(4)

[0114] 验证者的签名验证步骤

[0115] 接下来，将描述验证者执行的过程。首先，验证者从签名者获取电子签名 σ、电子文件 m、以及验证密钥 pk。然后，如果有必要，则验证者通过认证授权中心的证书对验证密钥 pk 是否是签名者的有效验证密钥进行验证。此后，验证者将验证密钥 pk、电子文件 m 和电子签名 σ 输入到签名验证算法 (Ver) 中并计算验证结果 $v_{out} = 0$（出错）还是 1（接受）。通过 Ver 计算 v_{out} 如下面的公式 (5) 所示。然后，验证者根据下面的公式 5 所计算的验证结果 v_{out}，在 $v_{out} = 1$ 的情况下接受 (σ, m) 并在 $v_{out} = 0$ 的情况下拒绝它们。在使用替代验证密钥 pk′ 执行验证过程时，执行同样的处理。

[0116] $v_{out} = Ver(pk, m, \sigma)$...(5)

[0117] 如上所述，在这些方案中，通过签名者与替代密钥生成者之间的交互，生成了接受使用签名密钥 sk 生成的电子文件 m 的电子签名 σ 的替代验证密钥 pk′。如此前所提到的，这些方案最初并非设计为了实施密钥更新方法而是用于允许签名者以外的实体（替代密钥生成者）安全地生成替代密钥。因此，与有效签名者的交互是替代密钥生成的要求，以

使得不随意地生成替代密钥。为此，在替代密钥生成步骤中，使用了关注输入信息种类的交互方法。

[0118] 1-4：替代验证密钥的属性

[0119] 在此，将通过参照图 4 对替代验证密钥 pk′ 的属性进行简要概述。如此前所提到的，替代验证密钥 pk′ 被配置成接受使用某个签名密钥 sk 生成的电子签名 σ 以及其上附加有该电子签名 σ 的电子文件 m。因此，替代验证密钥 pk′ 是针对电子文件 m 和电子签名 σ 对而生成的。当然，替代验证密钥 pk′ 不同于与签名密钥 sk 成对的验证密钥 pk。

[0120] 此外，替代验证密钥 pk′ 必须保证至少如下要求。要求 1：通过与签 名者的交互生成替代验证密钥 pk′ 的能力。要求 2：替代密钥生成者以外的人生成替代验证密钥的不可行性。通过这些要求，能够生成替代验证密钥 pk′ 的实体被限制为能够与签名者交互的实体。换言之，可以赋予能够与签名者交互的实体以生成替代密钥的能力。

[0121] 要求 3：替代密钥生成者无法伪造签名者的电子签名。即，作为要求来保证替代密钥生成者即使利用交互过程中获取的信息也不能伪造签名者的电子签名。通过此要求，可以确保签名者的电子签名不能被伪造。要求 4：签名者不能伪造替代密钥生成者的电子签名。即，作为要求来保证签名者即使利用交互过程中获取的信息也不能伪造使用与替代验证密钥 pk′ 成对的替代签名密钥 sk′ 生成的电子签名 σ′ 。通过此要求，可以确保替代密钥生成者的电子签名不能被伪造。

[0122] 通过满足上述要求 1 至 4，可以确保使用替代密钥的电子签名系统的安全性。接下来，下面将对满足这些要求的 SC08 方案的替代密钥生成方法以及具体算法进行描述。

[0123] 1-5：SC08 方案的替代密钥生成方法

[0124] 首先，参照图 5。图 5 是图示了 SC08 方案的替代密钥生成算法 <ORG(sk)，SUB> 中的大致处理流程的图。如图 5 中所示，假设验证密钥 pk、电子文件 m、以及电子签名 σ 被输入作为签名者与替代密钥生成者之间共享的信息。此外，在签名者一侧还使用签名密钥 sk。然而，为了使替代密钥生成者不能伪造签名者的电子签名，签名密钥 sk 不直接提供给替代密钥生成者。

[0125] 首先，替代密钥生成者生成替代签名密钥 sk′ ，并且使用关于替代签名密钥 sk′ 的信息生成替代验证密钥 pk′ 的局部信息。如以上所提到的，替代验证密钥 pk′ 将会接受用签名密钥 sk 生成的电子签名 σ 。为此，没有签名密钥 sk 的信息的替代密钥生成者在未获知关于签名密钥 sk 的信息的情况下不能生成替代验证密钥 pk′ 。此外，替代验证密钥 pk′ 将会接受用替代签名密钥 sk′ 生成的电子签名 σ′ （σ′ ≠ σ）。为此，替代验证密钥 pk′ 有必要包括关于替代签名密钥 sk′ 的信息。因此，如上所述，替代密钥生成者生成替代验证密钥 pk′ 中所包括的局部信息。

[0126] 将替代密钥生成者所生成的替代验证密钥 pk′ 中所包括的局部信息从替代密钥生成者提供给签名者 (S12)。然后，在获取替代验证密钥 pk′ 的局部信息后，签名者生成随机数并将随机数提供给替代密钥生成者 (S14)。 在从签名者获取随机数后，替代密钥生成者将关于使用所获取的随机数生成替代验证密钥 pk′ 所需要的替代签名密钥 sk′ 的信息提供给签名者 (S16)。如以上所提到的，替代验证密钥 pk′ 必须接受用替代签名密钥 sk′ 生成的电子签名 σ′ 。为此，有必要将关于替代签名密钥 sk′ 的信息提供给签名者。

[0127] 然而，当签名者获知了替代签名密钥 sk′ 时，将会随意生成用替代签名密钥 sk′

生成的电子签名 σ′ 。因此，替代密钥生成者以一种方式将关于替代签名密钥 sk′ 的信息提供给签名者以使得可以用签名者未识别的替代签名密钥 sk′ 使用随机数生成替代验证密钥 pk′ 。在获取关于替代签名密钥 sk′ 的这种信息后，签名者生成替代验证密钥 pk′ （在实践中，用于确定替代验证密钥 pk′ 的信息）(S18)。然后，签名者将生成的替代验证密钥 pk′ 提供给替代密钥生成者。即，根据 SC08 方案，虽然使用了术语替代密钥生成者，但是实际上替代验证密钥 pk′ 是由签名者生成的。

[0128] 通过上述方法，生成了替代签名密钥 sk′ 和替代验证密钥 pk′ 。在上文中，通过参照图 5，对 SC08 方案的替代密钥生成过程的大致流程进行了描述。然而，在以上描述中没有呈现具体运算方法。接下来，将对用于实施图 5 中所示的每个处理步骤的内容的具体运算算法进行详细描述。此处，应当注意，下面所给出的具体运算公式等只是示范性的并且可以按各种方式进行修改。

[0129] 1-6 :SC08 方案的算法

[0130] 首先，在对替代密钥生成算法的具体运算内容进行描述以前，将依次对根据 SC08 方案的系统参数生成算法、密钥生成算法、签名生成算法、以及签名验证算法进行描述。这些算法彼此相关并且包括用于实施替代密钥生成算法的 SC08 方案的特性配置。此后，将对替代密钥生成算法进行描述。

[0131] 系统参数生成算法

[0132] 首先，将通过参照图 6 对以上公式 1 所给出的系统参数生成算法进行描述。图 6 是图示了系统参数生成算法的具体运算内容的示例的图。系统参数生成算法由系统管理员执行。

[0133] 在系统参数生成算法中，首先，对于质数 $q = 3 \pmod 4$，选取满足下面的公式 6 的 λ 位质数 p(S30)。然后，选取阶数为 p 的 Z_p^* 的元素 g(S32)。此处，Z_p 表示模为质数 p 的整数的有限域，Z_p^* 表示其乘法群。此后，建 立包括质数 p 和元素 g 的系统参数 cp = (g, p)(S34)。这是系统参数生成算法的内容。当以此方式生成系统参数 cp 时，系统管理员将系统参数 cp 提供给每个实体 (S36)。在以下描述中，将假设系统参数 cp 提供给了每个实体。

[0134] $p = 2q+1 \ldots (6)$

[0135] 密钥生成算法和签名生成算法

[0136] 接下来，将通过参照图 7 对以上公式 2 所给出的密钥生成算法以及以上公式 3 所给出的签名生成算法进行描述。图 7 是图示了密钥生成算法和签名生成算法的具体运算内容的示例的图。密钥生成算法和签名生成算法由签名者执行。

[0137] 首先，将对密钥生成算法进行描述。在密钥生成算法中，首先随机选取 Z_q 的元素 x1 和 x2(S40)。然后，使用所选取的元素 x1 和 x2，通过下面的公式 7 和公式 8 计算 y1 和 y2(S42)。然后，随机选取 Z_q^* 的元素 α (S44)。此后，随机选取 $\{0,1\}^\lambda$ 的元素 w(S46)。可以适当地改变步骤 S44 和步骤 S46 的处理次序。这是密钥生成算法的内容。通过以上运算，生成了下面的公式 9 所给出的验证密钥 pk 以及下面的公式 10 所给出的签名密钥 sk。

[0138] $y1 = g^{x1} \bmod p \ldots (7)$

[0139] $y2 = g^{x2} \bmod p \ldots (8)$

[0140] $pk = (y1, y2, \alpha, w) \ldots (9)$

[0141] $sk = (x1, x2, \alpha)$...(10)

[0142] 接下来，将对签名生成算法进行描述。如以上公式 3 所给出的，在签名生成算法中，输入密钥生成算法所生成的签名密钥 sk 以及电子文件 m。在此情形中，由于已经计算了验证密钥 pk，因此验证密钥 pk 可以包括在输入值中。在以这种方式改变输入值时，如果签名生成算法中包括与以上公式 7 或 8 所给出的 y1 或 y2 相同的运算公式，则不必执行相应的运算处理。在以下描述中，与公式 7 和公式 8 相同的运算公式的部分将分别表示为 y1 和 y2。

[0143] 在签名生成算法中，首先随机选取 Z_q^* 的元素 k1(S50)。然后，使用所选取的元素 k1，计算下面的公式 11 所给出的 r1(S52)。然后，使用 r1、x1、以及 x2，计算下面的公式 12 所给出的 k2(S54)。此处，h3(…) 是散列函数。散列函数是根据某个比特序列 $a \in \{0,1\}$ 生成预定范围的数值的函数。此外，通过将某个比特序列应用于散列函数所得到的值称为散列值。在下面的公式 12 中，作为参数给出的值 r1、x1、以及 x2 例如彼此连接，并随后被输入到散列函数 h3 中。应当注意，在输入参数时执行的处理不限于连接。

[0144] 然后，使用所计算的 k2，计算下面的公式 13 所给出的 r2(S56)。此后，使用其上附加有电子签名 σ 的电子文件 m、通过上述运算计算得到的参数 r1 和 r2、以及验证密钥 pk 中所包括的参数 y1 和 y2(可以根据 x1 和 x2 生成)，计算下面的公式 14 和公式 15 所给出的参数 c 和 d(S58)。此处，h1(…) 和 h2(…) 都是散列函数。此外，参数 m、r1、r2、y1、以及 y2 例如彼此连接，并随后被输入到散列函数中。应当注意，在输入参数时执行的处理不限于连接。

[0145] 然后，使用计算得到的参数 c 和 d，计算下面的公式 16 和公式 17 所给出的 y 和 r(S60)。此后，使用步骤 S50 至步骤 S60 中获得的参数，计算 Z_q 满足下面的公式 18 的元素 s(S62)。此处，H(…) 是散列函数。此外，参数 c、r、以及 y 例如彼此连接，并随后被输入到散列函数中。应当注意，在输入参数时执行的处理不限于连接。通过以上运算，得到下面的公式 19 所给出的电子签名 σ。

[0146] $r1 = g^{K1} \bmod p$...(11)

[0147] $k2 = h3(r1, x1, x2)$...(12)

[0148] $r2 = g^{k2} \bmod p$...(13)

[0149] $c = h1(m, r1, r2, y1, y2, w)$...(14)

[0150] $d = h2(m, r1, r2, y1, y2, w)$...(15)

[0151] $y = y1 \cdot y2^{c} \bmod p$...(16)

[0152] $r = r1 \cdot r2^{d} \bmod p$...(17)

[0153] $H(c, r, y) = (x1+c \cdot x2)r \cdot \alpha + (k1+d \cdot k2)y \cdot s$...(18)

[0154] $\sigma = (r1, r2, s)$...(19)

[0155] 签名验证算法

[0156] 接下来，将通过参照图 8 对以上公式 5 所给出的签名验证算法进行描述。图 8 是图示了签名验证算法的具体运算内容的示例的图。签名验证算 法由验证者执行。

[0157] 首先，验证者获取公开的验证密钥 pk(见公式 9)(S70)。此外，验证者从签名者获取电子签名 σ(见公式 19)和电子文件 m(S72)。验证者将所获取的这些信息输入到签名验证算法中以对电子签名 σ 进行验证。另外，将假设验证者已经获取了系统参数 cp。

[0158] 在签名验证算法中，首先，基于以上的公式 14、15、16 以及 17 计算参数 c、d、y 以及 r(S74)。然后，将计算得到的参数代入到下面的公式 20 所给出的验证公式 A 中，从而对验证公式 A 是否有效进行验证 (S76 和 S78)。如果验证公式 A 有效，则该电子签名 σ 被视为有效，输出表示“接受”的输出值 $v_{out} = 1$(S80)，并且一系列处理结束。另一方面，如果验证公式 A 无效，则输出表示“错误”的输出值 $v_{out} = 0$(S82)，并且一系列处理结束。通过以上运算，验证了针对电子文件 m 的电子签名 σ 的有效性。

[0159] (SC08 方案)

[0160] $g^{H(c,r,y)} = y^{r \cdot q} \cdot r^{y \cdot s} \bmod p$

[0161] … (20)

[0162] SC08 方案的思想

[0163] 可以说电子签名方案是由验证公式的形式确定的。另外，验证公式 A 是特定于 SC08 方案的。验证公式 A 是通过对下面的公式 21 所给出的 ElGamal 签名方案的验证公式进行改进而导出的。在 ElGamal 签名方案的情形中，在将阶数为 q 的 Z_p^* 的元素 g 用作系统参数时，其中，质数 q 和 p 满足关系 $p = 2 \times q+1$ 和 $q = 3 \pmod 4$，只存在一个接受电子文件 m 和电子签名 σ 对的验证密钥 pk。为此，当签名生成系统基于 ElGamal 签名方案的验证公式构建时，不能生成替代密钥。即，不满足上述要求 1。因此，设计了以上公式 20 所给出的 SC08 方案的验证公式 A。在下文中，将对 SC08 方案的思想进行更详细的描述。

[0164] (ElGamal 签名方案)

[0165] 电子签名：$\sigma = (r, s)$、$r = g^k \bmod p$、

[0166] 签名密钥：$sk = x \in Z_p^*$、

[0167] 验证密钥：$pk = y = g^x \bmod p$、

[0168] 验证公式：$g^{H(m,r)} = y^r \cdot r^s \bmod p$

[0169] … (21)

[0170] 首先，在 SC08 方案中，添加了验证密钥 pk 的元素并修改了验证公式。此时，将能够通过与有效签名者的交互生成替代密钥的要求 (1) 以及在不与有效签名者交互的情况下不能生成替代验证密钥的要求 (2) 考虑在内。即，进行修改以满足要求 (1) 和要求 (2)。

[0171] Sakumoto 等人注意到了 ElGamal 签名方案具有如下属性：“即使在给出验证密钥的情况下也不能运算出满足验证公式的电子签名”。此外，通过参考 ElGamal 签名方案的属性以及以上公式 21 所给出的验证公式，Sakumoto 等人注意到了如下属性：如果验证公式中出现的电子签名的元素 r 与验证密钥的元素 y 是对称的，则“即使在给出电子签名的情况下也不能运算出满足验证公式的电子签名”。表述“对称”是指‘b’位于‘a’的斜上方（指数部分）并且‘a’位于‘b’的斜上方（指数部分）的形式 $(a^b \times b^a)$。

[0172] 因此，Sakumoto 等人基于此思想如下面的公式 22 所示向验证密钥 pk 添加了参数 α，并且如下面的公式 23 所示修改了验证公式。通过验证密钥 pk 中添加的参数 α，可以生成替代密钥。然而，在使用基于下面的公式 22 所给出的验证密钥 pk 其为有效的下面的公式 23 的验证公式时，替代密钥生成者将能够计算出原始的签名密钥 sk。例如，使用替代签名密钥 $sk' = x'$ 和替代验证密钥 $pk' = (y', \alpha')$，由于替代密钥生成者将能够获知下面的公式 24，因此基于此公式替代密钥生成者能够计算出应当由签名者秘密持有的参数 k。另外，由于替代密钥生成者使用原始的签名密钥 $sk = x$ 获知下面的公式 25 是有效的，

因此替代密钥生成者能够使用参数 k 根据下面的公式 25 计算出签名密钥 sk。

[0173] $pk = (y, \alpha)$...(22)

[0174] $g^{H(m,r,y)} = y^{r \cdot \alpha} \cdot r^{y \cdot s} \bmod p$...(23)

[0175] $H(m,r,y') = x' \cdot r \cdot \alpha + k \cdot y' \cdot s \bmod q$...(24)

[0176] $H(m,r,y) = x \cdot r \cdot \alpha + k \cdot y \cdot s \bmod q$...(25)

[0177] 因此，Sakumoto 等人如以上公式 9 和公式 10 所给出的将签名密钥 sk 和验证密钥 pk 中所包括的参数加倍，以使得替代密钥生成者不能生成原始的签名密钥 sk。当然，替代签名密钥 sk′ 和替代验证密钥 pk′ 中所包括的参数也加倍。此外，在 SC08 方案中，将签名者不能获知替代密钥生成者秘密持有的替代签名密钥 sk′ 的要求（以上要求 4）也考虑在内。关 于替代密钥的要求 3 和要求 4 通过后面所描述的替代密钥生成算法来实现。下文中将对体现该思想的 SC08 方案的替代密钥生成算法进行描述。

[0178] 替代密钥生成算法

[0179] 将通过参照图 9 对以上公式 4 所给出的替代密钥生成算法进行描述。图 9 是图示了替代密钥生成算法的具体运算内容的示例的图。替代密钥生成算法基于交互协议并且通过签名者与替代密钥生成者之间的交互来实现。

[0180] 在替代密钥生成算法中，首先签名者输入签名密钥 sk(S100)。在此情形中，签名密钥 sk 不直接提供给替代密钥生成者。此外，替代密钥生成者随机选取 Z_q 的元素 x1′ 和 x2′，并且计算下面的公式 26 和公式 27 所给出的 y1′ 和 y2′ (S102)。值 x1′ 和 x2′ 是替代签名密钥 sk′ 中包括的参数。此外，值 y1′ 和 y2′ 是替代验证密钥 pk′ 中包括的参数。然后，将参数 y1′ 和 y2′ 从替代密钥生成者提供给签名者 (S104)。此后，签名者随机选取 Z_q 的元素 w′ (S106)。然后，将元素 w′ 从签名者提供给替代密钥生成者 (S108)。

[0181] 在获取值 w′ 后，替代密钥生成者使用所获取的值 w′ 计算下面的公式 28 所给出的 c′ 以及下面的公式 29 所给出的 z(S110)。然后，将值 z 从替代密钥生成者提供给签名者 (S112)。应当注意，虽然值 z 包括构成替代签名密钥 sk′ 的一部分的参数 x1′ 和 x2′，但是值 z 以不单独确定参数 x1′ 和 x2′ 的方式提供给签名者。此后，在获取值 z 后，签名者基于以上公式 14、公式 15、公式 16、以及公式 17 计算 c、d、y、以及 r，并且计算满足下面的公式 30 的 k。在许多情形中，签名者不在其中持有参数 k1 和 k2。为此，在此步骤中，重新计算参数 k1 和 k2。

[0182] 当然，如果其中持有参数 k1 和 k2，则可以省略这些运算。然后，签名者使用以上的公式 12 计算 k2 并且通过将所计算的值 k 和 k2 代入到下面的公式 31 中计算 k1 在此步骤中，得到了参数 k1 和 k2。此后，签名者基于下面的公式 28 计算 c′。另外，签名者基于下面的公式 32 计算 d′。然后，签名者基于下面的公式 33 和公式 34 计算 y′ 和 r′。另外，签名者使用所计算的值 y′ 验证下面的公式 35 是否有效。此时，如果公式 35 无效，则签名者输出错误并且一系列处理结束。

[0183] 然后，签名者计算满足下面的公式 36 的 α′ (S114)。此外，将参数 α′ 从签名者提供给替代密钥生成者。通过组合参数 α′ 以及参数 y1′、y2′ 和 w′，生成替代验证密钥 pk′。如果参数 α′ 包括在替代签名密钥 sk′ 中，则此时还生成替代签名密钥 sk′。另外，可以构建以使得签名者生成替代验证密钥 pk′ 并将其提供给替代签名者。在 SC08 方案中，通过上述方法，生成替代验证密钥 pk′ 和替代签名密钥 sk′。

[0184] $y1' = g^{x1'} \bmod p$(26)

[0185] $y2' = g^{x2'} \bmod p$(27)

[0186] $c' = h1(m, r1, r2, y1', y2', w')$...(28)

[0187] $z = x1' + c' \cdot x2' \bmod q$...(29)

[0188] $H(c, r, y) = (x1+c \cdot x2)r \cdot \alpha + k \cdot y \cdot s \bmod q$...(30)

[0189] $k1 = k - d \cdot k2 \bmod q$...(31)

[0190] $d' = h2(m, r1, r2, y1', y2', w')$...(32)

[0191] $y' = y1' \cdot y2'^{c'} \bmod p$...(33)

[0192] $r' = r1 \cdot r2^{d'} \bmod p$...(34)

[0193] $y' = g^{z} \bmod p$...(35)

[0194] $H(c', r', y') = z \cdot r' \cdot \alpha' + (k1+d' \cdot k2)y' \cdot s \bmod q$...(36)

[0195] 在上文中，已经详细描述了 SC08 方案。此处，应当注意，签名者能够在替代密钥生成者获得替代验证密钥 pk′ 之前在交互过程中获得生成替代验证密钥 pk′ 所需要的足够的信息（见图 5）。这意味着，在通过替代验证密钥 pk′ 确定替代密钥生成者之前，存在替代签名密钥 sk′ 的局部信息泄漏给攻击者的可能性。结果，SC08 方案没有针对替代密钥生成者所确定的替代验证密钥 pk′ 保证关于电子签名的不可伪造的安全性。

[0196] 下面将提供对此问题的进一步描述。在以下理想化情况下，构成关于 SC08 方案的安全性的部分基础的 ElGamal 签名方案所保证的安全性得以保证。其中所提到的理想化情况是指如下情况：“如果签名者首先生成公共密钥 pk，然后签名者将公共密钥 pk 传递给攻击者，并且最终攻击者能够生成接受公共密钥 pk 的电子签名，则攻击者取得成功”。鉴于攻击者难以在此理想化情况中获胜，ElGamal 签名方案的安全性得以保证。换言之，在这些要求中的任何要求未满足的情况中，不保证安全性。然而，SC08 方案具有攻击者能够在签名者获知签名者的公共密钥之前获知公共密钥的构造。为此，基于 ElGamal 签名方案的签名方案可能会处于 ElGamal 签名方案所保证的安全性保证范围之外。

[0197] 为了解决上述问题，本发明人向 SC08 方案引入了额外的思想并且根据后面所描述的实施例设计了替代密钥生成方法。这些实施例的技术解决了上述问题并且提供了比 SC08 方案更高效的替代密钥生成方法。在下文中，将对根据本发明的实施例的替代密钥生成方法进行详细描述。

[0198] 2：第一实施例

[0199] 首先，将对本发明的第一实施例进行描述。本实施例解决了关于 SC08 方案安全性的问题并且涉及如下技术：在替代密钥生成者只确定了替代验证密钥 pk′ 的一部分的阶段，防止将估算包括替代验证者在后面生成的替代验证密钥 pk′ 的剩余部分的全部信息所需要的足够信息提供给签名者。即，虽然签名者能够生成替代验证密钥 pk′ 以外的替代验证密钥，但是在替代密钥生成者在生成替代验证密钥 pk″ 时只确定了替代验证密钥 pk′ 的一部分的状态下，防止签名者早于替代验证者获知包括剩余部分的替代验证密钥 pk′ 的全部。在下文中，将对此技术（本方案 1）进行详细描述。

[0200] 2-1：替代密钥生成方法

[0201] 首先，参照图 10。图 10 是图示了本方案 1 的替代密钥生成算法 <ORG(sk),SUB> 中的大致处理流程的图。如图 10 中所示，假设验证密钥 pk、电子文件 m、以及电子签名 σ 被

输入作为签名者与替代密钥生成者之间共享的信息。此外，在签名者一侧还使用签名密钥 sk。然而，为了使替代密钥生成者不能伪造签名者的电子签名，签名密钥 sk 不直接提供给替代密钥生成者。

[0202] 首先，替代密钥生成者生成替代签名密钥 sk′，并且使用关于替代签名密钥 sk′ 的信息生成替代验证密钥 pk′ 的局部信息。将替代密钥生成者所生成的替代验证密钥 pk′ 中所包括的局部信息从替代密钥生成者提供给签名者 (S122)。然而，在此步骤中提供的局部信息是不足以估算最终得到的替代验证密钥 pk′ 的信息。

[0203] 然后，在获取替代验证密钥 pk′ 的局部信息后，签名者生成随机数并将生成替代验证密钥 pk′ 所需要的关于签名密钥 sk 的信息连同随机数一起提供给替代密钥生成者 (S124)。然而，在此步骤中提供的关于签名密钥 sk 的信息是不足以使替代密钥生成者估算签名密钥 sk 的信息。在获取关于签名密钥 sk 的信息后，替代密钥生成者生成替代验证密钥 pk′ (S126)。

[0204] 通过上述方法，生成了替代签名密钥 sk′ 和替代验证密钥 pk′ 。以这种方式，在本方案 1 中，替代密钥生成者生成了替代验证密钥 pk′ 。此外，在替代密钥生成者确定替代验证密钥 pk′ 之前，生成替代验证密钥 pk′ 所需要的足够信息不提供给签名者。为此，通过使用本方案 1，解决了 SC08 方案的上述问题。然而，在以上描述中没有呈现具体运算方法。接下来，将对用于实施图 10 中所示的每个处理步骤内容的具体运算算法进行详细描述。此处，应当注意，下面所给出的具体运算公式式等只是示范性的并且可以按各种方式进行修改。

[0205] 2-2 :算法

[0206] 首先，在对替代密钥生成算法的具体运算内容进行描述以前，将依次描述根据本方案 1 的系统参数生成算法、密钥生成算法、签名生成算法、以及签名验证算法。由于系统参数生成算法基本上与 SC08 方案的相同，因此将省略其描述。此外，这些算法彼此相关并且包括用于实施替代密钥生成算法的 SC08 方案的特性配置。此后，将对替代密钥生成算法进行描述。

[0207] 密钥生成算法和签名生成算法

[0208] 首先，将通过参照图 11 对以上公式 2 所给出的密钥生成算法以及以上公式 3 所给出的签名生成算法进行描述。图 11 是图示了密钥生成算法和签名生成算法的具体运算内容的示例的图。密钥生成算法和签名生成算法由签名者执行。

[0209] 首先，将对密钥生成算法进行描述。在密钥生成算法中，首先随机选取 Z_q 的元素 x1 和 x2(S130)。然后，使用所选取的元素 x1 和 x2，通过下面的公式 37 和公式 38 计算 y1 和 y2(S132)。然后，随机选取 Z_q^* 的元素 α (S134)。可以适当地改变步骤 S134 的处理次序。这是密钥生成算法的内容。通过以上运算，生成了下面的公式 39 所给出的验证密钥 pk 以及下面的公式 40 所给出的签名密钥 sk。

[0210] $y1 = g^{x1} \bmod p \ldots (37)$

[0211] $y2 = g^{x2} \bmod p \ldots (38)$

[0212] $pk = (y1, y2, \alpha) \ldots (39)$

[0213] $sk = (x1, x2, \alpha) \ldots (40)$

[0214] 接下来，将对签名生成算法进行描述。如以上公式 3 所给出的，在签 名生成算法

中，输入密钥生成算法所生成的签名密钥 sk 以及电子文件 m。在此情形中，由于已经计算了验证密钥 pk，因此验证密钥 pk 可以包括在输入值中。在以这种方式改变输入值时，如果签名生成算法中包括与以上公式 37 或 38 所给出的 y1 或 y2 相同的运算公式，则不必执行相应的运算处理。在以下描述中，与公式 37 和公式 38 相同的运算公式的部分将分别用 y1 和 y2 表示。

[0215] 在签名生成算法中，首先随机选取 Z_q^* 的元素 k1(S140)。然后，使用所选取的元素 k1，计算下面的公式 41 所给出的 r1(S142)。然后，使用 r1、x1、以及 x2，计算下面的公式 42 所给出的 k2(S144)。此处，h3(…) 是散列函数。在下面的公式 42 中，作为参数给出的值 r1、x1、以及 x2 例如彼此连接，并且随后被输入到散列函数 h3 中。应当注意，在输入参数时执行的处理不限于连接。

[0216] 然后，使用所计算的 k2，计算下面的公式 43 所给出的 r2(S146)。此后，使用其上附加有电子签名 σ 的电子文件 m、通过上述运算所计算的参数 r1 和 r2、以及验证密钥 pk 中所包括的参数 y1 和 y2(可以根据 x1 和 x2 生成)，计算下面的公式 44 和公式 45 所给出的参数 c 和 d(S148)。此处，h1(…) 和 h2(…) 都是散列函数。此外，参数 m、r1、r2、y1、以及 y2 例如彼此连接，并且随后被输入到散列函数中。应当注意，在输入参数时执行的处理不限于连接。

[0217] 然后，使用所计算的参数 c 和 d，计算下面的公式 46 和公式 47 所给出的 y 和 r(S150)。此后，使用步骤 S130 至步骤 S150 中所得到的参数，计算 Z_q 满足下面的公式 48 的元素 s(S152)。此处，H(…) 是散列函数。此外，参数 c、r、以及 y 例如彼此连接，并且随后被输入到散列函数中。应当注意，在输入参数时执行的处理不限于连接。通过以上运算，获得下面的公式 49 所给出的电子签名 σ。

[0218] $r1 = g^{k1} \bmod p \ldots (41)$

[0219] $k2 = h3(r1, x1, x2) \ldots (42)$

[0220] $r2 = g^{k2} \bmod p \ldots (43)$

[0221] $c = h1(m, r1, r2, y1, y2) \ldots (44)$

[0222] $d = h2(m, r1, r2, y1, y2) \ldots (45)$

[0223] $y = y1 \cdot y2^{c} \bmod p \ldots (46)$

[0224] $r = r1 \cdot r2^{d} \bmod p \ldots (47)$

[0225] $H(c, r, y) = (x1+c \cdot x2)r \cdot \alpha + (k1+d \cdot k2)y \cdot s \bmod q \ldots (48)$

[0226] $\sigma = (r1, r2, s) \ldots (49)$

[0227] 在上文中，对根据本方案 1 的密钥生成算法和签名生成算法进行了描述。在密钥生成算法中，所生成的验证密钥 pk 的构造相对于 SC08 方案的有所改变。另一方面，在签名生成算法中，用于生成电子签名 σ 的参数 c 和 d 的构造相对于 SC08 方案的有所改变。特别地，应当注意，输入到散列函数 h2 中的参数种类在生成参数 d 时发生了改变。这一改变来自于如下事实：从替代密钥生成者提供给签名者的信息比 SC08 方案的少。换言之，通过这种改变，可以减少从替代密钥生成者提供给签名者的信息量。

[0228] 签名验证算法

[0229] 接下来，将通过参照图 12 对以上公式 5 所给出的签名验证算法进行描述。图 12 是图示了签名验证算法的具体运算内容的示例的图。签名验证算法由验证者执行。

[0230] 首先，验证者获取公开的验证密钥 pk（见公式 39）(S160)。此外，验证者从签名者获取电子签名 σ（见公式 49）和电子文件 m(S162)。验证者将所获取的这些信息输入到签名验证算法中以对电子签名 σ 进行验证。另外，假设验证者已经获取了系统参数 cp。

[0231] 在签名验证算法中，首先基于以上公式 44、45、46、以及 47 计算参数 c、d、y、以及 r(S164)。然后，将所计算的参数代入到下面的公式 50 所给出的验证公式 A 中，从而对验证公式 A 是否有效进行验证 (S166 和 S168)。如果验证公式 A 有效，则该电子签名 σ 被视为有效，输出表明

[0232] “接受”的输出值 $v_{out} = 1$(S170)，并且一系列处理结束。另一方面，如果验证公式 A 无效，则输出表明错误的输出值 $v_{out} = 0$(S172)，并且一系列处理结束。通过以上运算，验证了针对电子文件 m 的电子签名 σ 的有效性。此处，应当注意，根据本方案 1 的验证公式 A 的形式显示为与 SC08 方案的相同。

[0233] （本方案 1）

[0234] $g^{H(c,r,y)} = y^{r \cdot q} \cdot r^{y \cdot s} \bmod p$

[0235] …(50)

[0236] 替代密钥生成算法

[0237] 接下来，将通过参照图 13 对以上公式 4 所给出的替代密钥生成算法进行描述。图 13 是图示了替代密钥生成算法的具体运算内容的示例的图。替代密钥生成算法基于交互协议并且通过签名者与替代密钥生成者之间的交互来实现。然而，与 SC08 方案不同，在本方案 1 中，替代验证密钥是在替代密钥生成者一侧生成的。

[0238] 在替代密钥生成算法中，首先签名者输入签名密钥 sk(S180)。在此情形中，签名密钥 sk 不直接提供给替代密钥生成者。此外，替代密钥生成者随机选取 Z_q 的元素 x1′，并且计算下面的公式 51 所给出的参数 y1′ (S182)。然后，将参数 y1′ 从替代密钥生成者提供给签名者 (S184)。应当注意，即使利用步骤 S184 中提供给签名者的参数 y1′ 签名者也不能生成替代验证密钥。此后，签名者随机选取 Z_q 的元素 w(S186)。

[0239] 然后，签名者基于以上公式 44、公式 45、公式 46、以及公式 47 计算 c、d、y、以及 r，并且计算满足下面的公式 52 的 k。在许多情形中，签名者不在其中持有参数 k1 和 k2。为此，在此步骤中重新计算参数 k1 和 k2。当然，如果其中持有参数 k1 和 k2，则可以省略这些运算。

[0240] 然后，签名者使用以上公式 42 计算 k2 并且通过将所计算的值 k 和 k2 代入到下面的公式 53 中计算 k1。在此步骤中，得到了参数 k1 和 k2。此后，签名者基于下面的公式 54 计算 d″。另外，签名者基于下面的公式 55 计算 k″ (S186) 并且将值 k″ 连同随机数 w 一起提供给替代密钥生成者 (S188)。应当注意，根据签名者在此阶段所持有的信息，不能估算替代密钥生成者最终生成的替代验证密钥。

[0241] 在从签名者获取随机数 w 和参数 k″ 后，替代密钥生成者随机选取 Z_q 的元素 x2″。然后，替代密钥生成者使用从签名者获取的随机数 w 以及所选取的参数 x1′ 计算下面的公式 56 所给出的参数 x1″。另外，替代密钥生成者基于下面的公式 57 和公式 58 计算参数 y1″ 和 y2″。从而所得到的参数 x1″ 和 x2″ 包括在替代签名密钥 sk″ 中。此外，参数 y1″ 和 y2″ 包括在替代验证密钥 pk″ 中。

[0242] 然后，替代密钥生成者使用其上附加有替代验证密钥 pk″ 要接受的电子签名 σ

的电子文件m、电子签名σ中所包括的参数r1和r2、以及要包括在替代验证密钥pk″中的参数y1″和y2″，通过下面的公式59计算参数c″。另外，替代密钥生成者基于下面的公式54计算预定的d″。此时，可以构造以使得代替y1′ w，可以将y1″代入到散列函数h2中。此后，替代密钥生成者基于下面的公式60和公式61计算参数y″和r″。

[0243] 此外，替代密钥生成者使用目前所得到的参数d″验证下面的公式61是否有效以及是否$w \in Z_q^*$。如果这些条件中的任何条件不满足，则与替代密钥生成算法相关联的一系列处理结束。如果两个条件都满足，则替代密钥生成者计算满足下面的公式63的参数α″ (S190)并且确定下面的公式64和公式65所分别给出的替代验证密钥pk″和替代签名密钥sk″。通过上述方法，生成了替代验证密钥pk″和替代签名密钥sk″。

[0244] 如以上所提到的，在本方案1中，从替代密钥生成者提供给签名者的信息只有参数y1′。为此，在替代密钥生成者确定替代验证密钥pk″之前签名者不能获得估算替代验证密钥pk″所需要的足够信息。因此，替代密钥生成者以外的人能够在确定替代验证密钥pk″之前估算出替代验证密钥pk″的SC08方案的问题得以解决。

[0245] 此外，在本方案1的情形中，减少了交互过程中签名者与替代密钥生成者之间的通信次数以及通信数据量。在图9中所示的SC08方案的替代密钥生成算法的情形中，发生了两次往返交互。此外，如果假设安全性参数的数据大小为a，则在SC08方案中在交互过程中的通信数据的大小为5×a。该数据由从替代密钥生成者发送给签名者的三个参数y1′、y2′、和z以及从签名者发送给替代密钥生成者的两个参数w′和α′组成。

[0246] 另一方面，在图13中所示的本方案1的替代密钥生成算法的情形中，只有一次往返交互。另外，在本方案1中在交互过程中的通信数据的大小仅为3×a。该数据由从替代密钥生成者发送给签名者的一个参数y1′以及从签名者发送给替代密钥生成者的两个参数w和k′组成。此外，当SC08方案的替代验证密钥pk′与本方案1的替代验证密钥pk″相比较时，替代验证密钥pk′的数据大小为4×a，而替代验证密钥pk″的数据大小仅为3×a。

[0247] 从以上可以看出，本方案1比SC08方案更高效，并且从通信负荷和替代验证密钥的数据大小的角度来看，本方案1优于SC08方案。

[0248] $y1' = g^{x1'} \bmod p$(51)

[0249] $H(c,r,y) = (x1+c \cdot x2)r \cdot \alpha + k \cdot y \cdot s \bmod q$...(52)

[0250] $k1 = k - d \cdot k2 \bmod q$...(53)

[0251] $d'' = h2(m,r1,r2,y1'^{w})$...(54)

[0252] $k'' = k1 + d'' \cdot k2 \bmod q$...(55)

[0253] $x1'' = x1' \cdot w \bmod q$...(56)

[0254] $y1'' = y1'^{w} \bmod p$...(57)

[0255] $y2'' = g^{x2''} \bmod p$(58)

[0256] $c'' = h1(m,r1,r2,y1'',y2'')$...(59)

[0257] $y'' = y1'' \cdot y2''^{c''} \bmod p$...(60)

[0258] $r'' = r1 \cdot r2^{d''} \bmod p$...(61)

[0259] $y'' = g^{k''} \bmod p$...(62)

[0260] $H(c'',r'',y'') = (x1'' + c'' \cdot x2'')r'' \cdot \alpha'' + k'' \cdot y'' \cdot s \bmod q$...(63)

[0261] $pk'' = (y1'', y2'', \alpha'')$...(64)

[0262] $sk'' = (x1'', x2'', \alpha'')$...(65)

[0263] 2-3：终端的功能配置

[0264] 此处，将通过参照图 14 对能够执行上述算法的本方案 1 的系统配置进行简要描述。参照图 14，示出了签名者所使用的签名者终端 100、验证者所使用的验证者终端 200、以及替代密钥生成者所使用的替代密钥生成者终端 300 的功能配置。此外，将假设签名者终端 100、验证者终端 200、以及替代密钥生成者终端 300 连接到网络 10。此处，没有示出系统管理员和认证授权中心的终端。

[0265] 签名者终端 100

[0266] 首先，将对签名者终端 100 的功能配置进行描述。如图 14 中所示，签名者终端 100 主要包括存储单元 102、密钥生成单元 104、签名生成单元 106、通信单元 108、以及签名密钥相关信息生成单元 110。

[0267] 存储单元 102 是用于存储系统参数 cp、电子文件 m、以及用于执行每个算法的程序的装置。密钥生成单元 104 从存储单元 102 中读取系统参数 cp 以及密钥生成算法的执行程序并且生成签名密钥 sk 和验证密钥 pk。密钥生成单元 104 所生成的签名密钥 sk 和验证密钥 pk 输入到签名生成单元 106 中。

[0268] 签名生成单元 106 从存储单元 102 中读取系统参数 cp 以及签名生成算法的执行程序，并且生成将使用所输入的签名密钥 sk（验证密钥 pk）附加到电子文件 m 上的电子签名 σ 以及电子文件 m。通信单元 108 将签名生成单元 106 所生成的电子签名 σ 和电子文件 m 经由网络 10 提供给验证者终端 200。

[0269] 签名密钥相关信息生成单元 110 是用于在替代密钥生成时生成随机数 w 并且计算用于生成替代验证密钥 pk'' 的参数 k'' 的装置。首先，签名密钥相关信息生成单元 110 从替代密钥生成者终端 300（具体地，替代验证密钥生成单元 306）获取关于替代验证密钥 pk'' 的参数 y1' 并且使用参数 y1' 生成参数 k''。此外，签名密钥相关信息生成单元 110 将参数 k'' 和 w 提供给替代密钥生成者终端 300。

[0270] 从以上可以看出，签名者终端 100 在其上配备了用于执行将由签名者根据本方案 1 执行的算法的功能。结果，通过使用签名者终端 100，实现了根据本方案的密钥更新方法。

[0271] 验证者终端 200

[0272] 接下来，将对验证者终端 200 的功能配置进行描述。如图 14 中所示，验证者终端 200 主要包括通信单元 202、参数生成单元 204、存储单元 206、以及验证处理单元 208。在存储单元 206 中，除了系统参数 cp，还存储了要由验证者执行的算法的执行程序。

[0273] 当通信单元 202 经由网络 10 从签名者终端 100 获取了电子文件 m 和电子签名 σ 时，这些电子文件 m 和电子签名 σ 被输入到参数生成单元 204 中。在参数生成单元 204 中，计算需要输入到验证公式中的参数。将参数生成单元 204 所计算的参数输入到验证处理单元 208 中。在验证处理单元 208 中，将参数生成单元 204 所计算的参数、验证密钥 pk、电子文件 m、以及电子签名 σ 输入到验证公式中，并且基于验证公式的有效性确定对电子签名 σ 的接受 / 拒绝。

[0274] 从以上可以看出，验证者终端 200 在其上配备了用于执行将由验证者根据本方案执行的算法的功能。结果，通过使用验证者终端 200，实现了根据本方案的密钥更新方法。

[0275] 替代密钥生成者终端 300

[0276] 接下来，将对替代密钥生成者终端 300 的功能配置进行描述。如图 14 中所示，替代密钥生成者终端 300 主要包括存储单元 302、替代签名密钥生成单元 304、替代验证密钥生成单元 306、以及通信单元 308。在存储单元 302 中，除了系统参数 cp，还存储了要由替代密钥生成者执行的算法的执行程序。

[0277] 替代签名密钥生成单元 304 在生成替代密钥时读取存储单元 302 中存储的系统参数 cp 并且生成关于替代签名密钥 sk″ 的参数 x1′ 和 x2″ 。替代 签名密钥生成单元 304 所生成的参数 x1′ 和 x2″ 输入到替代验证密钥生成单元 306 中。此外，当生成替代签名密钥 sk″ 所必需的足够的信息从替代验证密钥生成单元 306 输入时，替代签名密钥生成单元 304 使用该信息生成替代签名密钥 sk″ 。

[0278] 当参数 x1′ 和 x2″ 从替代签名密钥生成单元 304 输入时，替代验证密钥生成单元 306 基于替代验证密钥生成算法执行与签名者终端 100(具体地，签名密钥相关信息生成单元 110) 的交互并且获取足够用于生成替代验证密钥 pk″ 的参数 k″ 和 w。在此交互过程中，替代验证密钥生成单元 306 只将参数 y1′ 作为关于替代验证密钥 pk″ 的信息提供给签名者终端 100。为此，在此阶段，签名者终端 100 不能估算后面所确定的替代验证密钥 pk″ 。

[0279] 在从签名者终端 100 获取参数 k″ 和 w 后，替代验证密钥生成单元 306 使用参数 k″ 和 w 生成替代验证密钥 pk″ 。将在此生成步骤中计算的将要被包括在替代签名密钥 sk″ 中的参数从替代验证密钥生成单元 306 输入到替代签名密钥生成单元 304 中。此外，通信单元 308 经由网络 10 将替代验证密钥生成单元 306 所生成的替代验证密钥 pk″ 提供给验证者终端 200。虽然在图 14 中没有清楚地图示，但是替代密钥生成者终端 300 还可以包括例如用于使用替代签名密钥 sk″ 生成电子签名的签名生成装置。

[0280] 在上文中，对根据本方案 1 的替代密钥生成方法进行了描述。通过使用本方案 1，可以实现比 SC08 方案具有更高安全性和更高效率的密钥可替代电子签名系统。应当注意，以上描述中所呈现的具体运算内容可以在符合本方案 1 思想的范围内任意地改变。当然，改变后的运算内容也落入本方案 1 的技术范围内。

[0281] 3 :第二实施例

[0282] 接下来，将描述本发明的第二实施例。与第一实施例类似，本实施例解决了关于 SC08 方案的安全性的问题并且实现了如下技术 :“在替代密钥生成者只确定了替代验证密钥 pk′ 的一部分的阶段，防止将估算包括替代验证者在后面生成的替代验证密钥 pk′ 的剩余部分的全部信息所需要的足够信息提供给签名者”。

[0283] 然而，本实施例的方法包括不同的思想，在于将关于替代验证密钥 pk″ 的信息以使该信息保密的方式从替代密钥生成者提供给签名者。下文中，将详细描述该技术 (本方案 2)。本方案 2 与本方案 1 有共同的基本 技术思想，因此图 10 中所示的替代密钥生成方法的大致流程以及用于实现根据本方案 2 的替代密钥生成方法的终端配置基本上与本方案 1 的相同。因此，将省略对这些重复部分的描述。

[0284] 3-1 :算法

[0285] 首先，在对替代密钥生成算法的具体运算内容进行描述以前，将依次描述根据本方案 2 的系统参数生成算法、密钥生成算法、签名生成算法、以及签名验证算法。由于系统参数生成算法基本上与 SC08 方案的相同，将省略其描述。此外，这些算法彼此相关并且包

括用于实施替代密钥生成算法的本方案 2 的特性配置。此后，将对替代密钥生成算法进行描述。

[0286] 密钥生成算法和签名生成算法

[0287] 首先，将通过参照图 15 对以上公式 2 所给出的密钥生成算法以及以上公式 3 所给出的签名生成算法进行描述。图 15 是图示了密钥生成算法和签名生成算法的具体运算内容的示例的图。密钥生成算法和签名生成算法由签名者执行。

[0288] 首先，将对密钥生成算法进行描述。在密钥生成算法中，首先随机选取 Z_q 的元素 x1 和 x2(S200)。然后，使用所选取的元素 x1 和 x2，通过以上公式 37 和公式 38 计算 y1 和 y2(S202)。然后，随机选取 Z_q^* 的元素 α (S204)。可以适当地改变步骤 S204 的处理次序。这是密钥生成算法的内容。通过以上运算，生成了以上公式 39 所给出的验证密钥 pk 以及以上公式 40 所给出的签名密钥 sk。从以上可以看出，本方案 2 的密钥生成算法与本方案 1 的相同。

[0289] 接下来，将描述签名生成算法。如以上公式 3 所给出的，在签名生成算法中，输入密钥生成算法所生成的签名密钥 sk 以及电子文件 m。在此情形中，由于已经计算了验证密钥 pk，因此验证密钥 pk 可以包括在输入值中。在以这种方式改变输入值时，如果签名生成算法中包括与以上公式 37 或 38 所给出的 y1 或 y2 相同的运算公式，则不必执行相应的运算处理。在以下描述中，与公式 37 和公式 38 相同的运算方公式的部分将分别用 y1 和 y2 表示。

[0290] 在签名生成算法中，首先随机选取 Z_q^* 的元素 k1(S210)。然后，使用所选取的元素 k1，计算以上公式 41 所给出的 r1(S212)。然后，使用 r1、x1、以及 x2，计算以上公式 42 所给出的 k2(S214)。然后，使用所计算的 k2，计算以上公式 43 所给出的 r2(S216)。到目前为止的处理步 骤与本方案 1 的相同。

[0291] 然后，使用参数 y2 计算下面的公式 66 所给出的 Y，同时，使用其上附加有电子签名 σ 的电子文件 m、通过上述运算计算得到的参数 r1 和 r2、以及验证密钥 pk 中所包括的参数 y1 和 y2(可以根据 x1 和 x2 生成)，计算以上公式 44 和以下公式 67 所给出的参数 c 和 d(S218)。此处，h4(…) 是散列函数。从以上可以看出，在本方案 2 中引入了新的参数 Y。

[0292] 然后，使用计算得到的参数 c 和 d，计算以上公式 46 和公式 47 所给出的 y 和 r(S220)。此后，使用步骤 S200 至步骤 S220 中所得到的参数，计算 Z_q 满足以上公式 48 的元素 s(S222)。通过以上运算，获得了以上公式 49 所给出的电子签名 σ。

[0293] $Y = h4(y2) \ldots (66)$

[0294] $d = h2(m, r1, r2, y1, Y) \ldots (67)$

[0295] 在上文中，对根据本方案 2 的密钥生成算法和签名生成算法进行了描述。如以上所提到的，在本方案 2 中，在生成参数 d 时引入了新的参数 Y。如以上公式 66 所给出的，该参数 Y 是关于替代验证密钥 pk″ 的信息。此处，应当注意，参数 y2 转换成了散列值。转换成散列值的原因将在对替代密钥生成算法的描述中给出。

[0296] 从以上公式 48 可以理解，参数 d 确保了应当由签名者保密的参数 k1 和 k2 是不被确定的。在本方案 1 中，在生成参数 d 时只有参数 y1 被用作关于替代验证密钥 pk″ 的信息。另一方面，在本方案 2 中，除了参数 y1，还包括关于参数 y2 的参数 Y。为此，通过使用本方案 2，可以提高参数 k1 和 k2 的安全性，这是因为为了确定参数 d 所应当获知的信息量

增加。

[0297] 签名验证算法

[0298] 接下来，将通过参照图 16 对以上公式 5 所给出的签名验证算法进行描述。图 16 是图示了签名验证算法的具体运算内容的示例的图。签名验证算法由验证者执行。

[0299] 首先，验证者获取公开的验证密钥 pk（见公式 39）(S230)。此外，验证者从签名者获取电子签名 σ（见公式 49）和电子文件 m(S232)。验证者将所获取的这些信息输入到签名验证算法中以对电子签名 σ 进行验证。另外，将假设验证者已经获取了系统参数 cp。

[0300] 在签名验证算法中，首先基于以上公式 44、66、以及 67 计算参数 c、Y、以及 d，并且基于以上公式 46 和公式 47 计算参数 y 和 r(S234)。然后，将所计算的参数代入到以上公式 50 所给出的验证公式 A 中，从而对验证公式 A 是否有效进行验证 (S236 和 S238)。此处，应当注意，本方案 2 中使用与本方案 1 中所使用的相同的验证公式 A。

[0301] 如果验证公式 A 有效，则该电子签名 σ 被视为有效，输出表示“接受”的输出值 v_{out} ＝ 1(S240)，并且一系列处理结束。另一方面，如果验证公式 A 无效，则输出表示错误的输出值 v_{out} ＝ 0(S242)，并且一系列处理结束。通过以上运算，验证了针对电子文件 m 的电子签名 σ 的有效性。

[0302] 替代密钥生成算法

[0303] 接下来，将通过参照图 17 对以上公式 4 所给出的替代密钥生成算法进行描述。图 17 是图示了替代密钥生成算法的具体运算内容的示例的图。替代密钥生成算法基于交互协议并且通过签名者与替代密钥生成者之间的交互来实现。与本方案 1 类似，在本方案 2 中，替代验证密钥是在替代密钥生成者一侧生成的。

[0304] 在替代密钥生成算法中，首先签名者输入签名密钥 sk(S250)。在此情形中，签名密钥 sk 不直接提供给替代密钥生成者。此外，替代密钥生成者随机选取 Z_q 的元素 x1′ 和 x2″，并且计算下面的公式 68 和公式 69 所给出的参数 y1′ 和 y2″。另外，基于下面的公式 70 计算参数 Y″ (S252)。然后，将参数 y1′ 和 Y″ 从替代密钥生成者提供给签名者 (S254)。

[0305] 与本方案 1 不同，在本方案 2 中，在步骤 S254 中将关于替代验证密钥 pk″ 中所包括的两个参数 y1′ 和 y2″ 的信息提供给签名者。可以通过签名者所提供的参数 w 生成替代验证密钥 pk″ 中所包括的参数 y1″。为此，看起来与 SC08 方案中所使用的相同的两个参数 y1″ 和 y2″ 被传递给签名者。然而，由于将参数 y2″ 转换成了散列值 Y″，因此签名者不能根据散列值 Y″ 和参数 y1″ 生成替代验证密钥 pk″。即，确保了与本方案 1 相同的安全性。

[0306] 然而，在获取参数 y1′ 和 Y″ 后，签名者随机选取 Z_q 的元素 w。然后，签名者基于以上公式 44、公式 66、公式 67、公式 46、以及公式 47 计算 c、Y、d、y、以及 r，并且计算满足以上公式 52 的 k。在许多情形中，签名者不在其中持有参数 k1 和 k2。为此，在此步骤中，重新计算参数 k1 和 k2。当然，如果其中持有参数 k1 和 k2，则可以省略这些运算。

[0307] 然后，签名者使用以上公式 42 计算 k2 并且通过将计算得到的值 k 和 k2 代入到下面的公式 53 中计算 k1 在此步骤中，获得了参数 k1 和 k2。此后，签名者基于下面的公式 71 计算 d″。另外，签名者基于以上公式 55 计算 k″ (S256) 并且将值 k″ 连同随机数 w 一起提供给替代密钥生成者 (S258)。应当注意，根据签名者在此阶段所持有的信息，不能估算替代密钥生成者最终生成的替代验证密钥。

[0308] 在从签名者获取随机数 w 和参数 k″ 后，替代密钥生成者使用所获取的随机数 w 以及所选取的参数 x1′ 计算以上公式 56 所给出的参数 x1″ 。另外，替代密钥生成者基于以上公式 57 和公式 58 计算参数 y1″ 和 y2″ 。从而所得到的参数 x1″ 和 x2″ 包括在替代签名密钥 sk″ 中。此外，参数 y1″ 和 y2″ 包括在替代验证密钥 pk″ 中。

[0309] 然后，替代密钥生成者使用其上附加有替代验证密钥 pk″ 要接受的电子签名 σ 的电子文件 m、电子签名 σ 中所包括的参数 r1 和 r2、以及要包括在替代验证密钥 pk″ 中的参数 y1″ 和 y2″ ，通过以上公式 59 计算参数 c″ 。另外，替代密钥生成者基于以上公式 71 计算预定的 d″ 。此时，可以构造以使得代替 y1′ w，可以将 y1″ 代入到散列函数 h2 中。此后，替代密钥生成者基于以上公式 60 和公式 61 计算参数 y″ 和 r″ 。

[0310] 此外，替代密钥生成者使用目前所获得的参数 d″ 验证以上公式 61 是否有效以及是否 $w \in Z_q^*$ 。如果这些条件中的任何条件不满足，则与替代密钥生成算法相关联的一系列处理结束。如果两个条件都满足，则替代密钥生成者计算满足以上公式 63 的参数 α″ (S260) 并且确定以上公式 64 和公式 65 所分别给出的替代验证密钥 pk″ 和替代签名密钥 sk″ 。通过上述方法，生成了替代验证密钥 pk″ 和替代签名密钥 sk″ 。

[0311] 如以上所提到的，在本方案 2 中，从替代密钥生成者提供给签名者的信息只有参数 y1′ 和 Y″ 。然而，参数 Y″ 是关于替代验证密钥 pk″ 的信息 y2″ 的散列值。为此，在替代密钥生成者确定替代验证密钥 pk″ 之前签名者不能获得估算替代验证密钥 pk″ 所需要的足够信息。因此，替代密钥生成者以外的人能够在确定替代验证密钥 pk″ 之前估算替代验证密钥 pk″ 的 SC08 方案的问题得以解决。此外，本方案 2 也比 SC08 方案更高效。

[0312] $y1' = g^{x1'} \bmod p \ldots (68)$

[0313] $y2'' = g^{x2''} \bmod p \ldots (69)$

[0314] $Y'' = h4(y2'') \ldots (70)$

[0315] $d'' = h2(m, r1, r2, y1' \ w, Y'') \ldots (71)$

[0316] 4 :对第一和第二实施例的修改

[0317] 在上文中，对根据本发明第一和第二实施例的替代密钥生成方法进行了描述。然而，在以上描述中，只提到了用于生成接受签名者一侧准备的电子文件和电子签名对的替代密钥的方法。接下来，将对用于生成接受替代密钥生成者所准备的电子文件以及使用根据第一和第二实施例的替代密钥生成方法附加到电子文件上的电子密钥对的替代密钥的方法（在下文中称作本修改）进行简要描述。

[0318] 4-1 :替代密钥生成方法

[0319] 在下文中，将通过参照图 18 对根据本修改的替代密钥生成方法进行简要描述。如图 18 中所示，替代密钥生成者准备替代密钥生成者想要在其上附加电子签名的电子文件 m。此时，签名者还准备签名密钥 sk。首先，替代密钥生成者提供电子文件 m 以及替代验证密钥 pk′ 中所包括的局部信息 (S272)。此时提供的信息与本方案 1 和 2 中的相同。在获取该信息后，签名者使用签名者的签名密钥 sk 生成电子文件 m 的电子签名 σ (S274)。

[0320] 然后，签名者使用关于从替代密钥生成者获取的替代验证密钥 pk′ 的信息以及关于签名密钥 sk 的信息计算生成替代验证密钥 pk′ 所需要的信息并且将所计算的信息连同电子签名 σ 一起提供给替代密钥生成者 (S276)。在获取该信息和电子签名 σ 后，替代密钥生成者生成替代验证密钥 pk′ (S278)。通过执行这些处理，替代密钥生成者能够获得电

子文件 m 的电子签名 σ、接受电子文件 m 和电子签名 σ 的替代验证密钥 pk′、以及与替代验证密钥 pk′ 成对的替代签名密钥 sk′。

[0321] 使用这种配置，可以针对在替代密钥生成者一侧准备的电子文件 m 的电子签名 σ 生成替代密钥。可以根据本发明的方面适当地进行这种修改。从该修改可以理解，在依附本方案 1 和 2 所提出的技术范围的范围内，可以获得与本方案 1 和 2 相同的益处。因此，这种修改也属于根据本发明的第一和第二实施例的技术范围。

[0322] 5：终端的示范性硬件配置

[0323] 签名者终端 100、验证者终端 200、以及替代密钥生成者终端 300 的各组成元件的功能可以用例如图 19 中所示的图像处理装置的硬件配置来实现。即，通过使用计算机程序控制图 19 中所示的硬件实现组成元件的功能。硬件的形式是任意的并且可以包括诸如个人计算机、手机、PHS、PDA、游戏机、以及各种信息装置的移动信息终端。此处，PHS 是个人手持式电话系统的缩写。此外，PDA 是个人数字助理的缩写。

[0324] 如图 19 中所示，硬件主要包括 CPU 902、ROM 904、RAM 906、主机总线 908、以及桥接器 910。另外，硬件还包括外部总线 912、接口 914、输入单元 916、输出单元 918、存储单元 920、驱动器 922、连接端口 924、以及通信单元 926。此处，CPU 是中央处理单元的缩写。此外，ROM 是只读存储器的缩写。此外，RAM 是随机存取存储器的缩写。

[0325] CPU 902 用作例如运算处理单元和控制设备，并且基于 ROM 904、RAM 906、存储单元 920、以及可移除存储介质 928 中的至少一个中所存储的各种类型的程序控制各种组成元件的所有或部分操作。ROM 904 是用于存储例如运算中以及 CPU 902 所读取的程序所使用的数据等的装置。RAM 906 在其中暂时地或永久地存储例如 CPU 902 所读取的程序、在程序执行时根据需要变化的各种类型的参数等。

[0326] 这些组成元件通过例如能够用于高速数据传输的主机总线 908 互连。主机总线 908 通过桥接器 910 连接到数据传输速度相对较低的外部总线 912。此外，例如使用鼠标、键盘、触摸面板、按钮、开关、操纵杆等作为输入单元 916。另外，可以使用能够使用红外线或其它电磁波来发送控制信号的远程控制单元作为输入单元 916。

[0327] 可以使用诸如 CRT、LCD、PDP、或者 ELD 的显示设备，诸如扬声器或耳机的音频输出设备，传真机等作为输出单元 918。即，输出单元 918 是用于以视觉和听觉的方式将所获得的信息通知给用户的装置。此处，CRT 是阴极射线管的缩写。此外，LCD 是液晶显示器的缩写。另外，PDP 是等离子体显示面板的缩写。此外，ELD 是电致发光显示器的缩写。

[0328] 存储单元 920 是用于存储各种类型的数据的设备。例如可以使用诸如 HDD 的磁存储设备、半导体存储设备、光学存储设备和磁光存储设备等作为存储单元 920。此处，HDD 是硬盘驱动器的缩写。

[0329] 驱动器 922 是用于从 / 向可移除存储介质 928 读取或写入信息的设备，可移除存储介质 928 例如可以是磁盘、光盘、磁光盘或半导体存储器等。可移除存储介质 928 例如可以是 DVD 介质、蓝光介质、HD DVD 介质、以及各种类型的半导体存储介质。当然，可移除存储介质 928 可以是其上安装有非接触式 IC 芯片的 IC 卡、电子设备等。此处，IC 是集成电路的缩写。

[0330] 连接端口 924 是用于将外部连接设备 930 与其连接的端口，诸如 USB 端口、IEEE 1394 端口、SCSI 端口、RS-232C 端口、或者光学音频端子等。外部连接设备 930 例如可以是

打印机、便携式音乐播放器、数码相机、数码摄像机、IC 记录器等。此处，USB 是通用串行总线的缩写。此外，SCSI 是小型计算机系统接口的缩写。

[0331] 通信单元 926 是用于连接到网络 932 的通信设备，可以是例如用于有线或无线 LAN、蓝牙（注册商标）、或者 WUSB 的通信卡，用于光通信的路由器，用于 ADSL 的路由器，用于各种类型通信的调制解调器等。此外，连接到通信单元 926 的网络 932 是通过有线或无线方式连接的网络，可以是例如互联网、家庭 LAN、红外通信网络、可见光通信网络、广播网络或者卫星通信网络等。此处，LAN 是局域网的缩写。此外，WUSB 是无线 USB 的缩写。此外，ADSL 是非对称数字用户线路的缩写。

[0332] 6 :应用示例

[0333] 接下来，将对根据本发明的第一和第二实施例的替代密钥生成方法的应用示例进行描述。该替代密钥生成方法涉及一种生成接受针对电子文件 m 的使用签名密钥 sk 和验证密钥 pk 对生成的电子签名 σ 的替代验证密钥 pk″ 的方法。作为使用接受电子文件 m 和电子签名 σ 对 (m, σ) 的替代验证密钥 pk″ 的方法，可以考虑例如在签名密钥 sk 泄漏时用替代验证密钥 pk″ 和替代签名密钥 sk″ 替代签名密钥 sk 和验证密钥 pk 的密钥更新方法。

[0334] 此外，通过充分利用替代验证密钥 pk″ 的属性，可以考虑一种将替代密钥生成方法应用于后面将要描述的 PKI、代理签名方案等的方法。当然，替代密钥生成方法的应用范围不限于这些示例。为了帮助扩展替代密钥生成方法的应用范围，在此部分中，将介绍应用于 PKI、应用于代理签名方案和应用于角色共享电子签名作为具体示例。另外，根据第一和第二实施例的替代密钥生成方法的任何技术都可以应用于此部分中所介绍的应用示例。

[0335] 6-1 :应用于 PKI

[0336] 首先，将通过参照图 21 和图 22 对用于将根据第一和第二实施例的替代密钥生成方法应用于 PKI 的方法（下文中称作应用示例 1）进行描述。图 21 是示出了能够实现根据应用示例 1 的方法的 PKI 系统的示例的图。图 22 是示出了根据应用示例 1 的整个处理的流程的图。应用示例 1 将替 代密钥生成方法应用于基于认证授权中心的公共密钥（对应于验证密钥）的验证方法。

[0337] PKI（公共密钥基础设施）是如下方案 :认证授权中心 (CA) 检查拥有公共密钥 pk 的用户的 ID（身份）并且将用户的 ID 与公共密钥 pk 绑定。此处，CA 是认证授权中心的缩写。可以通过例如以下 6 套算法来说明应用示例 1 中的 PKI 方案。

[0338] (A1) 系统参数生成算法

[0339] (A2)CA 密钥生成算法

[0340] (A3) 密钥注册算法（交互协议）

[0341] (A4) 签名生成算法

[0342] (A5) 签名验证算法

[0343] (A6) 验证密钥验证算法

[0344] 系统参数生成算法 A1 由系统管理员使用并且对应于 SC08 方案中的系统参数生成算法 SetupKSS（见图 6）。

[0345] CA 密钥生成算法 A2 是由认证授权中心使用的算法并且生成由认证授权中心使用且对认证授权中心唯一的秘密密钥 sk 和公共密钥 pk 对。CA 密钥生成算法所生成的公共密

钥 pk 被公开以用于验证认证授权中心所发布的证书。CA 密钥生成算法所生成的秘密密钥 sk 由认证授权中心秘密管理。

[0346] 由认证授权中心秘密管理的秘密密钥 sk 用于生成后面所描述的用户验证密钥 pk″ 。此处，认证授权中心所发布的证书证明用户验证密钥 pk″ 与用户 ID 绑定。此外，CA 密钥生成算法对应于根据第一和第二实施例的密钥生成算法 GenKSS（见图 11 和图 15）。然而，应当注意，CA 密钥生成算法由认证授权中心而非前面的描述中所提到的签名者使用。

[0347] 密钥注册算法 A3 是生成用户所使用的用户验证密钥 pk″ 和用户的签名密钥 sk″ 并且生成用于证明用户验证密钥 pk″ 的有效性的证书的算法。密钥注册算法基于交互协议在认证授权中心与用户之间执行。密钥注册算法所生成的用户验证密钥 pk″ 被公开并且用于使用用户的签名密钥 sk″ 生成的电子签名的验证。

[0348] 此外，用户的签名密钥 sk″ 由用户秘密管理。此外，密钥注册算法对应于根据第一和第二实施例的替代密钥生成算法（见图 13 和图 17）。然 而，应当注意，密钥注册算法在认证授权中心与用户之间而非前面的描述中所提到的在签名者与替代签名者之间使用。

[0349] 签名生成算法 A4 是允许用户使用用户的签名密钥 sk″ 生成电子文件 m 的电子签名 σ 的算法。此外，签名生成算法对应于根据第一和第二实施例的签名生成算法 SigKSS（见图 11 和图 15）。然而，应当注意，签名生成算法由用户（对应于替代密钥生成者）使用。

[0350] 签名验证算法 A5 是对用户的电子签名 σ 是否是电子文件 m 的有效电子签名进行验证的算法。签名验证算法由验证用户的电子签名 σ 的验证者使用。这里所提到的签名验证算法对应于根据第一和第二实施例的签名验证算法 Ver（见图 12 和图 16）。

[0351] 验证密钥验证算法 A6 是对认证授权中心所发布的证书是否是有效证书进行验证并且还使用该证书验证用户验证密钥 pk″ 是否是有效验证密钥的算法。此处，将对验证密钥验证算法 A6 进行更详细的描述。

[0352] 如以上所提到的，根据第一和第二实施例的替代密钥生成算法是一种生成接受针对电子文件 m 的使用签名密钥 sk 和验证密钥 pk 对生成的电子签名 σ 的替代验证密钥 pk″ 的方法。在应用示例 1 中，签名密钥 sk 和验证密钥 pk 对应于认证授权中心所生成的秘密密钥 sk 和公共密钥 pk。此外，在应用示例 1 中，其中描述了用户 ID 的电子文件 m_{ID} 用作电子文件 m。此外，使用针对电子文件 m_{ID} 基于秘密密钥 sk 生成的电子签名 σ_{ID} 作为电子签名 σ 。

[0353] 然而，电子签名 σ_{ID} 用作认证授权中心所发布的用户验证密钥 pk″ 的证书。用户验证密钥 pk″ 对应于根据第一和第二实施例的替代密钥生成算法所生成的替代验证密钥 pk″ 。即，有效用户验证密钥 pk″ 接受针对电子文件 m_{ID} 生成的证书 σ_{ID}。相反，通过验证用户验证密钥 pk″ 是否接受 (m_{ID}, σ_{ID}) 对，可以验证用户验证密钥 pk″ 的有效性。

[0354] 此外，通过验证认证授权中心所发布的公共密钥 pk 是否接受 (m_{ID}, σ_{ID}) 对，可以判定证书 σ_{ID} 的有效性。以此方式，验证密钥验证算法 A6 通过验证认证授权中心所生成的公共密钥 pk 是否接受 (m_{ID}, σ_{ID}) 对以及基于交互协议生成的用户验证密钥 pk″ 是否接受 (m_{ID}, σ_{ID}) 对，对认证授权中心所发布的证书 σ_{ID} 以及用户验证密钥 pk″ 的有效性进行验证。

[0355] 在下文中，将对根据应用示例 1 的系统配置以及具体处理流程进行描述。

[0356] 系统配置

[0357] 首先，参照图21。如图21中所示，应用示例1的系统包括提供给认证授权中心的认证授权中心服务器130、验证者所使用的验证者终端230、以及用户所使用的用户终端330。此外，认证授权中心服务器130、验证者终端230、以及用户终端330通过网络10连接。这里没有示出系统管理员的配置。

[0358] 认证授权中心服务器130

[0359] 首先，将描述认证授权中心服务器130的功能配置。如图21中所示，认证授权中心服务器130主要包括存储单元132、密钥生成单元134、签名生成单元136、通信单元138、以及秘密密钥相关信息生成单元140。

[0360] 存储单元132是用于存储系统参数cp、电子文件m、以及用于执行每个算法的程序的装置。密钥生成单元134从存储单元132读取系统参数cp以及CA密钥生成算法的执行程序，并且生成秘密密钥sk和公共密钥pk。密钥生成单元134所生成的秘密密钥sk和公共密钥pk输入到签名生成单元136中。此外，公共密钥pk通过通信单元138公开，并且输入到验证者终端230中。当然，用户终端330也能够获取公共密钥pk。

[0361] 此外，签名生成单元136还接收电子文件m_{ID}，其中包括用于识别用户的用户ID。此处，秘密密钥sk和公共密钥pk对应于第一和第二实施例中的有效签名者所生成的签名密钥sk和验证密钥pk。签名生成单元136从存储单元132中读取系统参数cp以及签名生成算法的执行程序，并且生成将使用所输入的秘密密钥sk被附加到电子文件m_{ID}上的电子签名σ_{ID}以及电子文件m_{ID}。

[0362] 通信单元138将签名生成单元136所生成的电子签名σ_{ID}和电子文件m_{ID}经由网络10提供给验证者终端230。电子文件m_{ID}和电子签名σ_{ID}对用作后面所描述的用户验证密钥pk″的证书(m_{ID}, σ_{ID})。为此，公共密钥pk和证书(m_{ID}, σ_{ID})不从认证授权中心服务器130提供给验证者终端230。

[0363] 秘密密钥相关信息生成单元140是用于生成关于使用密钥注册算法生成用户验证密钥pk″所需要的秘密密钥sk的信息的装置。如以上所提到的，密钥注册算法是对应于根据第一和第二实施例的替代密钥生成算法的交互协议。为此，秘密密钥相关信息生成单元140从用户终端330(具体地，用户验证密钥生成单元336)获取生成关于秘密密钥sk的信息所 需要的信息并且使用所获取的信息生成关于秘密密钥sk的信息。

[0364] 例如，当使用与根据第一实施例的替代密钥生成算法(见图13)相对应的交互协议时，秘密密钥相关信息生成单元140生成随机数w并且计算用于生成替代验证密钥pk″的参数k″。另外，秘密密钥相关信息生成单元140从用户终端330(具体地，用户验证密钥生成单元336)获取关于用户验证密钥pk″的参数y1′并且使用参数y1′生成参数k″。

[0365] 将以此方式生成的参数k″和w从秘密密钥相关信息生成单元140提供给用户终端330。以此方式，在作为交互协议的密钥注册算法中，将生成用户验证密钥pk″所需要的信息从认证授权中心服务器130提供给用户终端330。

[0366] 验证者终端230

[0367] 接下来，将对验证者终端230的功能配置进行描述。如图21中所示，验证者终端230主要包括通信单元202、参数生成单元204、存储单元206、以及验证处理单元232。在存储单元206中，除了系统参数cp，还存储了要由验证者执行的算法的执行程序。在此示例

中，假设被认证授权中心公开的公共密钥 pk 也提前存储于存储单元 206 中。

[0368] 首先，通信单元 202 经由网络 10 从认证授权中心服务器 130 获取证书 (m_{ID}, σ_{ID})，并且证书 (m_{ID}, σ_{ID}) 被输入到参数生成单元 204 中。在参数生成单元 204 中，计算执行签名验证算法和验证密钥验证算法所需要的参数。将参数生成单元 204 所计算的参数输入到验证处理单元 232 中。

[0369] 随后，验证处理单元 232 首先将参数生成单元 204 所计算的参数、用户验证密钥 pk″、公共密钥 pk、以及证书 (m_{ID}, σ_{ID}) 输入到验证密钥验证算法中，从而验证证书的有效性以及用户验证密钥 pk″ 的有效性。当验证了信息的有效性时，验证处理单元 232 将参数生成单元 204 所计算的参数、用户验证密钥 pk″、以及用户所生成的电子文件 m 和电子签名 σ 输入到签名验证算法中，从而对电子签名 σ 的有效性进行验证。

[0370] 以此方式，在验证者终端 230 中，验证证书以及用户验证密钥的有效性。结果，可以判定 PKI 中用户的公共密钥所对应的用户验证密钥与用户 ID 所对应的电子文件 m_{ID} 之间的绑定。当判定该绑定时，使用用户验证密钥对电子签名进行验证。

[0371] 用户终端 330

[0372] 接下来，将对用户终端 330 的功能配置进行描述。如图 21 中所示，用户终端 330 主要包括存储单元 332、用户的签名密钥生成单元 334、用户验证密钥生成单元 336、通信单元 338、以及签名生成单元 340。在存储单元 332 中，除了系统参数 cp，还存储了要由替代密钥生成者执行的算法的执行程序。

[0373] 用户的签名密钥生成单元 334 是用于生成用户的签名密钥 sk″ 的装置。例如，当使用与根据第一实施例的密钥生成算法（见图 11）相同的算法时，用户的签名密钥生成单元 334 读取存储单元 332 中存储的系统参数 cp 并且生成与用户的签名密钥 sk″ 有关的参数 x1′ 和 x2″。

[0374] 随后，用户的签名密钥生成单元 334 将参数 x1′ 和 x2″ 输入到用户验证密钥生成单元 336 中。此外，在从用户验证密钥生成单元 336 接收到生成替代签名密钥 sk″ 所需要的信息后，用户的签名密钥生成单元 334 通过添加该信息生成替代签名密钥 sk″。将用户的签名密钥生成单元 334 所生成的用户的签名密钥输入到签名生成单元 340 中。

[0375] 在从用户的签名密钥生成单元 334 接收到参数 x1′ 和 x2″ 后，用户验证密钥生成单元 336 执行与认证授权中心服务器 130（具体地，秘密密钥相关信息生成单元 140）的交互并且获取生成替代验证密钥 pk″ 所需要的参数 k″ 和 w。此交互基于与根据第一和第二实施例的替代密钥生成算法相对应的密钥注册算法来执行。例如，当使用根据第一实施例的替代密钥生成算法所对应的密钥注册算法时，用户验证密钥生成单元 336 将参数 y1′ 作为替代验证密钥 pk″ 的信息提供给认证授权中心服务器 130。

[0376] 如以上所提到的，在接收到参数 y1′ 后，认证授权中心服务器 130 的秘密密钥相关信息生成单元 140 基于参数 y1′ 将生成用户验证密钥 pk″ 所需要的信息（例如，k″ 和 w）提供给用户验证密钥生成单元 336。此处，应当注意，在此阶段认证授权中心服务器 130 不能估算后面所确定的用户验证密钥 pk″。在从认证授权中心服务器 130 获取参数 k″ 和 w 后，用户验证密钥生成单元 336 使用参数 k″ 和 w 生成用户验证密钥 pk″。通信单元 338 经由网络 10 将用户验证密钥生成单元 336 所生成的用户验证密钥 pk″ 提供给验证者终端 230。

[0377] 在用户验证密钥 pk″ 的该生成步骤中计算得到的一部分参数可以包括在用户的签名密钥 sk″ 中。在这种情形中，在此阶段将用户的签名密钥 sk″ 中所包括的参数从用户验证密钥生成单元 336 输入到用户的签名密钥生成单元 334 中。如以上所提到的，用户的签名密钥生成单元 334 使用所输入的参数生成用户的签名密钥 sk″ 。此外，将用户的签名密钥生成单元 334 所生成的用户的签名密钥 sk″ 输入到签名生成单元 340 中。

[0378] 签名生成单元 340 是用于使用从用户的签名密钥生成单元 334 输入的用户的签名密钥 sk″ 生成用户的电子签名 σ 的装置。签名生成单元 340 使用签名生成算法生成电子文件 m 的电子签名 σ 。在此阶段所生成的电子文件 m 和电子签名 σ 将会被用户验证密钥生成单元 336 所生成的用户验证密钥 pk″ 接受。通信单元 338 将签名生成单元 340 所生成的电子文件 m 和电子签名 σ 对提供给验证者终端 230。

[0379] 在上文中，对应用示例 1 的系统配置进行了描述。接下来，将通过参照图 22 对根据应用示例 1 的公共密钥认证方法及其整个处理流程进行简要描述。

[0380] 公共密钥认证方法

[0381] 参照图 22。如上所述，在应用示例 1 中出现的实体主要由四个实体组成，即系统管理员、认证授权中心、用户、以及验证者。在图 22 中，将对除系统管理员之外的认证授权中心、用户、以及验证者所执行的过程进行描述。下面将对这些过程进行描述。

[0382] 认证授权中心的过程 :密钥生成步骤

[0383] 首先，将对认证授权中心所进行的密钥生成处理进行描述。认证授权中心从系统管理员获取系统参数 cp。然后，所获取的系统参数 cp 被输入到 CA 密钥生成算法中，并且生成秘密密钥 sk 和公共密钥 pk 对。此后，认证授权中心存储秘密密钥 sk 和公共密钥 pk 对。

[0384] 认证授权中心和用户的过程 :用户密钥生成步骤

[0385] 接下来，将对认证授权中心和用户所进行的用户密钥生成处理进行描述。首先，用户将他 / 她自身的用户 ID 提供给认证授权中心。然后，认证授权中心准备在密钥生成步骤中所生成的秘密密钥 sk 和公共密钥 pk 以及包括用户 ID 的电子文件 m_{ID}。此后，认证授权中心使用秘密密钥 sk 生成电子文件 m_{ID} 的电子签名 σ_{ID}。然后，认证授权中心将电子文件 m_{ID}、电子签名 σ_{ID}、以及公共密钥 pk 提供给用户。

[0386] 随后，用户从认证授权中心接收电子文件 m_{ID}、电子签名 σ_{ID}、以及公共密钥 pk。以此方式，当电子文件 m_{ID}、电子签名 σ_{ID}、以及公共密钥 pk 在认证授权中心与用户之间共享时，认证授权中心和用户将电子文件 m_{ID}、电子签名 σ_{ID}、以及公头密钥 pk 输入到与根据第一和第二实施例的替代密钥生成算法相对应的密钥注册算法中，从而以交互的方式生成用户验证密钥 pk″ 和用户的签名密钥 sk″ 。在此交互过程中，认证授权中心将关于秘密密钥 sk 的信息提供给用户同时防止用户确定秘密密钥 sk。

[0387] 验证者的过程 :签名验证步骤

[0388] 接下来，将对验证者所进行的签名验证过程进行描述。验证者从用户获取电子文件 m、电子签名 σ 、以及用户验证密钥 pk″ 。在此阶段所获取的电子签名 σ 是使用用户的签名密钥 sk″ 针对电子文件 m 生成的签名。然后，如果有必要，则验证者验证用户验证密钥 pk″ 的有效性。此时，验证者使用验证密钥验证算法、使用从认证授权中心获取的证书 (m_{ID}, σ_{ID}) 对用户验证密钥 pk″ 的有效性进行验证。当验证了用户验证密钥 pk″ 的有效性

时，验证者将用户验证密钥 pk″、电子文件 m、以及电子签名 σ 输入到签名验证算法中以对电子签名 σ 进行验证，从而判定电子签名 σ 的有效性。

[0389] 验证者的过程：验证密钥验证步骤

[0390] 接下来，将对验证者所进行的验证密钥验证过程进行描述。在签名验证步骤中，验证者使用验证密钥验证算法对用户验证密钥 pk″ 的有效性进行验证。在此部分中所描述的验证密钥验证步骤涉及此验证处理。首先，验证者从认证授权中心获取公共密钥 pk 并且准备用户验证密钥 pk″ 和证书 (m_{ID}, σ_{ID})。然后，验证者将用户验证密钥 pk″ 和证书 (m_{ID}, σ_{ID}) 输入到验证密钥验证算法中，从而验证用户验证密钥 pk″ 和证书 (m_{ID}, σ_{ID}) 的有效性。

[0391] 验证密钥验证算法通过采用根据第一和第二实施例的签名验证算法来实现。首先，为了验证证书 (m_{ID}, σ_{ID}) 的有效性，将认证授权中心的公共密钥 pk 和证书 (m_{ID}, σ_{ID}) 输入到签名验证算法中，并且随后确定验证公式是否有效。类似地，为了验证用户验证密钥 pk″ 的有效性，将用户验证密钥 pk″ 和证书 (m_{ID}, σ_{ID}) 输入到签名验证算法中，并且随后确定验证公式是否有效。即，验证密钥验证算法执行这些处理。当对于两个输入确定验证公式有效时，接受用户验证密钥 pk″。

[0392] 在上文中，描述了根据应用示例 1 的公共密钥认证方法。从以上可以看出，根据第一和第二实施例的替代密钥的属性可以应用于 PKI 中公共密钥（用户验证密钥）的认证。

[0393] 6-2：应用于代理签名方案

[0394] 接下来，将通过参照图 23 和图 24 对将根据第一和第二实施例的替代 密钥生成方法应用于代理签名方案的方法（下文中称作应用示例 2）进行描述。图 23 是示出了能够实现根据应用示例 2 的方法的代理签名系统的示例的图。图 24 是示出了根据应用示例 2 的整个处理的流程的图。

[0395] 代理签名方案是指使得委托人能够将其自身的签名生成能力的一部分传递给代理的电子签名方案。通过例如以下 6 套算法来说明代理签名方案。

[0396] (A1) 系统参数生成算法

[0397] (A2) 密钥生成算法

[0398] (A3) 代理密钥生成算法

[0399] (A4) 签名生成算法

[0400] (A5) 签名验证算法

[0401] (A6) 代理验证算法

[0402] 系统参数生成算法 A1 由系统管理员使用并对应于 SC08 方案中的系统参数生成算法 SetupKSS（见图 6）。

[0403] 密钥生成算法 A2 是由委托人使用并且生成用于由委托人使用并对委托人唯一的签名密钥 sk 和验证密钥 pk 对的算法。密钥生成算法所生成的验证密钥 pk 被公开以用于对使用签名密钥 sk 生成的电子签名 σ 进行验证。密钥生成算法所生成的签名密钥 sk 由委托人秘密管理。

[0404] 由委托人秘密管理的签名密钥 sk 用于生成后面所描述的替代验证密钥 pk″。此外，密钥生成算法对应于根据第一和第二实施例的密钥生成算法 GenKSS（见图 11 和图 15）。然而，应当注意，密钥生成算法由委托人而非签名者使用。

[0405] 代理密钥生成算法 A3 是生成代理所使用的替代验证密钥 pk″ 以及替代签名密钥 sk″、并且生成委托人使用的用于证明代理有效性的证书的算法。代理密钥生成算法基于交互协议在委托人与代理之间执行。代理密钥生成算法所生成的替代验证密钥 pk″ 被公开以用于对使用替代签名密钥 sk″ 生成的电子签名进行验证。

[0406] 此外，替代签名密钥 sk″ 由代理秘密管理。代理密钥生成算法对应于根据第一和第二实施例的替代密钥生成算法（见图 13 和图 17）。此外，代理密钥生成算法在委托人与代理之间而非在签名者与替代签名者之间使用。委托人的证书证明委托人承认了代理的替代验证密钥。

[0407] 签名生成算法 A4 是允许代理使用替代签名密钥 sk″ 生成电子文件 m 的电子签名 σ 的算法。此外，签名生成算法对应于根据第一和第二实施例的签名生成算法 SigKSS（见图 11 和图 15）。然而，应当注意，签名生成算法由委托人和代理这两者使用。

[0408] 签名验证算法 A5 是验证电子签名 σ 是否是电子文件 m 的有效电子签名的算法。签名验证算法由验证代理的电子签名 σ 的验证者或委托人使用。这里所提到的签名验证算法对应于根据第一和第二实施例的签名验证算法 Ver（见图 12 和图 16）。

[0409] 代理验证算法 A6 是验证代理是否是被委托人承认的有效代理的算法。为了验证代理的有效性，代理验证算法对委托人所发布的证书是否是有效证书进行验证并且还使用该证书对替代验证密钥 pk″ 是否是有效验证密钥进行证实。此处，将对代理验证算法 A6 进行更详细的描述。

[0410] 如以上所提到的，根据第一和第二实施例的替代密钥生成算法是一种生成接受针对电子文件 m 使用签名密钥 sk 和验证密钥 KV′ 对生成的电子签名 σ 的替代验证密钥 pk″ 的方法。在应用示例 2 中，签名密钥 sk 和验证密钥 pk 对应于委托人所生成的签名密钥 sk 和验证密钥 pk。此外，在应用示例 2 中，包括所传递的权限范围、有效期等的电子文件 m_w 用作电子文件 m。此外，使用针对电子文件 m_w 基于签名密钥 sk 生成的电子签名 σ_w 作为电子签名 σ。

[0411] 然而，电子签名 σ_w 用作委托人所发布的替代验证密钥 pk″ 的证书。替代验证密钥 pk″ 对应于根据第一和第二实施例的替代密钥生成算法所生成的替代验证密钥 pk″。即，有效替代验证密钥 pk″ 接受针对电子文件 m_w 生成的证书 σ_w。相反，通过验证替代验证密钥 pk″ 是否接受 (m_w, σ_w) 对，可以对代理的替代验证密钥 pk″ 是否被委托人承认进行验证。

[0412] 此外，通过对委托人所发布的验证密钥 pk 是否接受 (m_w, σ_w) 对进行验证，可以判定证书 σ_w 的有效性。以此方式，代理验证算法 A6 通过对委托人所生成的验证密钥 pk 是否接受 (m_w, σ_w) 对以及基于交互协议生成的替代验证密钥 pk″ 是否接受 (m_w, σ_w) 对进行验证，从而对委托人所发布的证书 σ_w 以及替代验证密钥 pk″ 的有效性进行验证。

[0413] 在下文中，将对根据应用示例 2 的系统配置以及具体处理流程进行描述。

[0414] 系统配置

[0415] 首先，参照图 23。如图 23 中所示，应用示例 2 的系统包括委托人所使用的委托人终端 150、验证者所使用的验证者终端 250、以及代理所使用的代理终端 350。此外，委托人终端 150、验证者终端 250、以及代理终端 350 通过网络 10 连接。此处，没有示出系统管理员的配置。

[0416] 委托人终端 150

[0417] 首先，将对委托人终端 150 的功能配置进行描述。如图 23 中所示，委托人终端 150 主要包括存储单元 152、密钥生成单元 154、签名生成单元 156、通信单元 158、以及签名密钥相关信息生成单元 160。

[0418] 存储单元 152 是用于存储系统参数 cp、电子文件 m、以及用于执行每个算法的程序的装置。密钥生成单元 154 从存储单元 152 中读取系统参数 cp 以及密钥生成算法的执行程序并且生成签名密钥 sk 和验证密钥 pk。密钥生成单元 154 所生成的签名密钥 sk 和验证密钥 pk 输入到签名生成单元 156 中。此外，验证密钥 pk 通过通信单元 158 公开，并且被输入到验证者终端 250 中。当然，代理终端 350 也能够获取验证密钥 pk。

[0419] 此外，签名生成单元 156 还接收电子文件 m_w，其中包括所传递的权限的范围、有效期等。此处，委托人的签名密钥 sk 和验证密钥 pk 对应于第一和第二实施例中的有效签名者所生成的签名密钥 sk 和验证密钥 pk。签名生成单元 156 从存储单元 152 中读取系统参数 cp 以及签名生成算法的执行程序并且生成将使用所输入的签名密钥 sk 被附加到电子文件 m_w 上的电子签名 σ_w 以及电子文件 m_w。

[0420] 通信单元 158 将签名生成单元 156 所生成的电子签名 σ_w 和电子文件 m_w 经由网络 10 提供给验证者终端 250。电子文件 m_w 和电子签名 σ_w 对用作用于证明委托人承认了替代验证密钥 pk″ 的证书 (m_w, σ_w)。为此，验证密钥 pk 和证书 (m_w, σ_w) 不从委托人终端 150 提供给验证者终端 250。

[0421] 签名密钥相关信息生成单元 160 是用于生成关于使用代理密钥生成算法生成替代验证密钥 pk″ 所需要的签名密钥 sk 的信息的装置。如以上所提到的，代理密钥生成算法是对应于根据第一和第二实施例的替代密钥生成算法的交互协议。为此，签名密钥相关信息生成单元 160 从代理终端 350（具体地，替代验证密钥生成单元 356）获取生成关于签名密钥 sk 的信息所需要的信息并且使用所获取的信息生成关于签名密钥 sk 的信息。

[0422] 例如，当使用根据第一实施例的替代密钥生成算法（见图 13）所对应的交互协议时，签名密钥相关信息生成单元 160 生成随机数 w 并且计 算用于生成替代验证密钥 pk″ 的参数 k″。另外，签名密钥相关信息生成单元 160 从代理终端 350（具体地，替代验证密钥生成单元 356）获取关于替代验证密钥 pk″ 的参数 y1′ 并且使用参数 y1′ 生成参数 k″。

[0423] 将以此方式生成的参数 k″ 和 w 从签名密钥相关信息生成单元 160 提供给代理终端 350。以此方式，在作为交互协议的代理密钥生成算法中，将生成替代验证密钥 pk″ 所需要的信息从委托人终端 150 提供给代理终端 350。

[0424] 验证者终端 250

[0425] 接下来，将对验证者终端 250 的功能配置进行描述。如图 23 中所示，验证者终端 250 主要包括通信单元 202、参数生成单元 204、存储单元 206、以及验证处理单元 252。在存储单元 206 中，除了系统参数 cp，还存储了要由验证者执行的算法的执行程序。在此示例中，将假设从委托人提供的验证密钥 pk 也提前存储于存储单元 206 中。

[0426] 首先，通信单元 202 经由网络 10 从委托人终端 150 获取证书 (m_w, σ_w)，并且证书 (m_w, σ_w) 被输入到参数生成单元 204 中。在参数生成单元 204 中，计算执行签名验证算法和代理验证算法所需要的参数。将参数生成单元 204 所计算的参数输入到验证处理单元 252 中。

[0427] 随后，验证处理单元252首先将参数生成单元204计算得到的参数、替代验证密钥pk″、验证密钥pk、以及证书 (m_w, σ_w) 输入到代理验证算法中，从而对代理的有效性和替代验证密钥pk″的有效性进行验证。当验证了信息的有效性时，验证处理单元252将参数生成单元204计算得到的参数、替代验证密钥pk″、以及用户所生成的电子文件m和电子签名σ输入到签名验证算法中，从而验证电子签名σ的有效性。以此方式，在验证者终端250中，对代理和电子签名进行验证。

[0428] 代理终端350

[0429] 接下来，将对代理终端350的功能配置进行描述。如图23中所示，代理终端350主要包括存储单元352、替代签名密钥生成单元354、替代验证密钥生成单元356、通信单元358、以及签名生成单元360。在存储单元352中，除了系统参数cp，还存储了要由替代密钥生成者执行的算法的执行程序。

[0430] 替代签名密钥生成单元354是用于生成替代签名密钥sk″的装置。例如，当使用与根据第一实施例的密钥生成算法（见图11）相同的算法时，替代签名密钥生成单元354读取存储单元352中存储的系统参数cp并且生成与替代签名密钥sk″有关的参数x1′和x2″。

[0431] 随后，替代签名密钥生成单元354将参数x1′和x2″输入到替代验证密钥生成单元356中。此外，在从替代验证密钥生成单元356接收到生成替代签名密钥sk″所需要的信息后，替代签名密钥生成单元354通过添加该信息生成替代签名密钥sk″。替代签名密钥生成单元354所生成的替代签名密钥输入到签名生成单元360中。

[0432] 在从替代签名密钥生成单元354接收到参数x1′和x2″后，替代验证密钥生成单元356执行与委托人终端150（具体地，签名密钥相关信息生成单元160）的交互并且获取生成替代验证密钥pk″所需要的参数k″和w。此交互基于根据第一和第二实施例的替代密钥生成算法所对应的代理密钥生成算法而执行。例如，当使用根据第一实施例的替代密钥生成算法所对应的代理密钥生成算法时，替代验证密钥生成单元356将参数y1′作为关于替代验证密钥pk″的信息提供给委托人终端150。

[0433] 如以上所提到的，在接收到参数y1′后，委托人终端150的签名密钥相关信息生成单元160基于参数y1′将生成替代验证密钥pk″所需要的信息（例如，k″和w）提供给替代验证密钥生成单元356。此处，应当注意，在此阶段，委托人终端150不能估算后面所确定的替代验证密钥pk″。在从委托人终端150获取参数k″和w后，替代验证密钥生成单元356使用参数k″和w生成替代验证密钥pk″。通信单元358经由网络10将替代验证密钥生成单元356所生成的替代验证密钥pk″提供给验证者终端250。

[0434] 该替代验证密钥pk″的生成步骤中所计算的一部分参数可以包括在替代签名密钥sk″中。在这种情形中，在此阶段将替代签名密钥sk″中所包括的参数从替代验证密钥生成单元356输入到替代签名密钥生成单元354中。如以上所提到的，替代签名密钥生成单元354使用所输入的参数生成替代签名密钥sk″。此外，替代签名密钥生成单元354所生成的替代签名密钥sk″输入到签名生成单元360中。

[0435] 签名生成单元360是用于使用从替代签名密钥生成单元354输入的替代签名密钥sk″生成代理的电子签名σ的装置。签名生成单元360使用签名生成算法生成电子文件m的电子签名σ。在此阶段所生成的电子文件m和电子签名σ将会被替代验证密钥生成

单元 356 所生成的替代验证密钥 pk″ 接受。通信单元 358 将签名生成单元 360 所生成的电子文件 m 和电子签名 σ 对提供给验证者终端 250。

[0436] 在上文中，对应用示例 2 的系统配置进行了描述。接下来，通过参照图 24，将对根据应用示例 2 的代理认证方法及其整个处理流程进行简要描述。

[0437] 代理认证方法

[0438] 参照图 24。如上所述，在应用示例 2 中出现的实体主要由四个实体组成，即系统管理员、委托人、代理、以及验证者。在图 24 中，将对除系统管理员之外的委托人、代理、以及验证者所执行的过程进行描述。下面将对这些过程进行描述。

[0439] 委托人的过程 :密钥生成步骤

[0440] 首先，将对委托人所进行的密钥生成处理进行描述。委托人从系统管理员获取系统参数 cp。然后，所获取的系统参数 cp 输入到密钥生成算法中，并且生成签名密钥 sk 和验证密钥 pk 对。此后，委托人存储签名密钥 sk 和验证密钥 pk 对。

[0441] 委托人和代理的过程 :替代密钥生成步骤

[0442] 接下来，将对委托人和代理所进行的替代密钥生成处理进行描述。首先，委托人准备密钥生成步骤中所生成的签名密钥 sk 和验证密钥 pk 以及包括所传递的代理权限、有效期等的电子文件 m_w。此后，委托人使用签名密钥 sk 生成电子文件 m_w 的电子签名 σ_w。然后，委托人将电子文件 m_w、电子签名 σ_w、以及验证密钥 pk 提供给代理。

[0443] 随后，代理从委托人接收电子文件 m_w、电子签名 σ_w、以及验证密钥 pk。以此方式，当电子文件 m_w、电子签名 σ_w、以及验证密钥 pk 在委托人与代理之间共享时，委托人和代理将电子文件 m_w、电子签名 σ_w、以及验证密钥 pk 输入到根据第一和第二实施例的替代密钥生成算法所对应的代理密钥生成算法中，从而以交互的方式生成替代验证密钥 pk″ 和替代签名密钥 sk″。在此交互过程中，委托人将关于签名密钥 sk 的信息提供给代理同时防止代理确定签名密钥 sk。

[0444] 验证者的过程 :签名验证步骤

[0445] 接下来，将对验证者所进行的签名验证处理进行描述。验证者从代理获取电子文件 m、电子签名 σ、以及替代验证密钥 pk″。在此阶段所获取的电子签名 σ 是代理使用替代签名密钥 sk″ 针对电子文件 m 生成的签名。然后，如果有必要，则验证者对替代验证密钥 pk″ 的有效性（即，代理的有效性）进行验证。此时，验证者使用代理验证算法、使用从委托人获取 的证书 (m_w, σ_w) 验证替代验证密钥 pk″ 的有效性进行。当验证了替代验证密钥 pk″ 的有效性时，验证者将替代验证密钥 pk″、电子文件 m、以及电子签名 σ 输入到签名验证算法中以对电子签名 σ 进行验证，从而判定电子签名 σ 的有效性。

[0446] 验证者的过程 :代理验证步骤

[0447] 接下来，将对验证者所进行的代理验证处理进行描述。在签名验证步骤中，验证者使用代理验证算法对替代验证密钥 pk″ 的有效性进行验证。在此部分中所描述的代理验证步骤涉及此验证处理。首先，验证者从委托人获取验证密钥 pk 并且准备替代验证密钥 pk″ 和证书 (m_w, σ_w)。然后，验证者将替代验证密钥 pk″ 和证书 (m_w, σ_w) 输入到代理验证算法中，从而对替代验证密钥 pk″ 和证书 (m_w, σ_w) 的有效性进行验证。

[0448] 代理验证算法通过采用根据第一和第二实施例的签名验证算法来实现。首先，为了对证书 (m_w, σ_w) 的有效性进行验证，将委托人的验证密钥 pk 和证书 (m_w, σ_w) 输入到签名

验证算法中，并随后确定验证公式是否有效。类似地，为了对替代验证密钥 pk″ 进行验证，将替代验证密钥 pk″ 和证书 (m_w, σ_w) 输入到签名验证算法中，并随后确定验证公式是否有效。即，代理验证算法执行这些处理。当针对两个输入确定验证公式有效时，接受替代验证密钥 pk″ 。

[0449] 在上文中，对根据应用示例 2 的公共密钥认证方法进行了描述。从以上可以看出，根据第一和第二实施例的替代密钥的属性可以应用于代理签名方案。

[0450] 6-3 :应用于角色共享电子签名

[0451] 接下来，将对应用于角色共享电子签名进行简要描述。在典型的电子签名方案中，只存在一个接受电子文件和电子签名对的验证密钥。为此，只有一个用户将会承担对于某对电子文件和电子签名的责任。然而，通过使用根据第一和第二实施例的替代密钥生成方法，可以生成接受电子文件和电子签名对的新的验证密钥（替代验证密钥）和签名密钥（替代签名密钥）对。为此，通过允许另一个用户生成替代验证密钥和替代签名密钥对，可以与其他用户共享对于某对电子文件和电子签名的责任。以此方式，通过使用根据第一和第二实施例的替代密钥生成方法，可以实现角色共享电子签名方案。

[0452] 虽然不是角色共享电子签名方案，但是关于使签名者不被识别的技 术，已知有 RONALD L. RIVEST 的如下报告（下文中称作环签名方案）。RONALD L.RIVESTAnd ADI SHAMIR And YAEL TAUMAN,“How to Leak a Secret”,Advances in Cryptology,ASIACRYPT 2001,7th International Conference on the Theory and Application of Cryptology and Information Security,Gold Coast,Australia,December 9-13,2001,Proceedings, Springer,Lecture Notes in Computer Science,Volume 2448.

[0453] 环签名方案涉及一种使得难以从多个选择的验证密钥的所有者中识别出谁是有效签名者的技术。为此，考虑将环签名方案应用于告密。通过使用环签名方案，可以“提前并首次”选择多个验证密钥并且生成电子签名（环签名）以被多个选择的验证密钥接受。对环签名的验证不是分别地使用各个选择的验证密钥来执行的，而是通过确定环签名是否被多个选择的验证密钥接受来执行的。即，环签名方案是由能够生成被多个验证密钥接受的环签名的专用签名算法以及用多个验证密钥对环签名进行验证的专用验证算法指定的。

[0454] 在根据第一和第二实施例的替代密钥生成算法中，签名生成算法是生成被一个验证密钥接受的电子签名的算法。此外，验证算法是用于对电子签名是否被一个验证密钥接受进行验证的算法。此外，替代密钥生成算法生成“在生成签名后作为参考项”接受电子签名的新验证密钥。因此，在生成一次电子签名之后，可以与其他用户共享对于该电子签名的责任。即使以任何方式修改环签名方案，也不能实现这种角色共享。在此部分中，仅作为参考，对根据第一和第二实施例的替代密钥生成算法与环签名方案之间的区别、以及根据这些实施例的技术的优势进行了描述。如上文中所述，根据第一和第二实施例的替代密钥生成算法可以以各种方式来应用。

[0455] 本申请包含与 2009 年 4 月 30 日提交于日本专利局的日本在先专利申请 JP 2009-111578 以及 2009 年 5 月 22 日提交于日本专利局的日本在先专利申请 JP 2009-124035 中所公开的主题相关的主题，日本在先专利申请 JP 2009-111578 和日本在先专利申请 JP 2009-124035 的全部内容通过引用合并于此。

[0456] 虽然已经示出和描述了本发明的优选实施例，但是本发明不限于所描述的实施

例。本领域的技术人员应当理解，可以根据设计要求和其它因素进行各种修改、组合、子组合和变换，只要这些修改、组合、子组合和变换在所附权利要求或其等价内容的范围内。

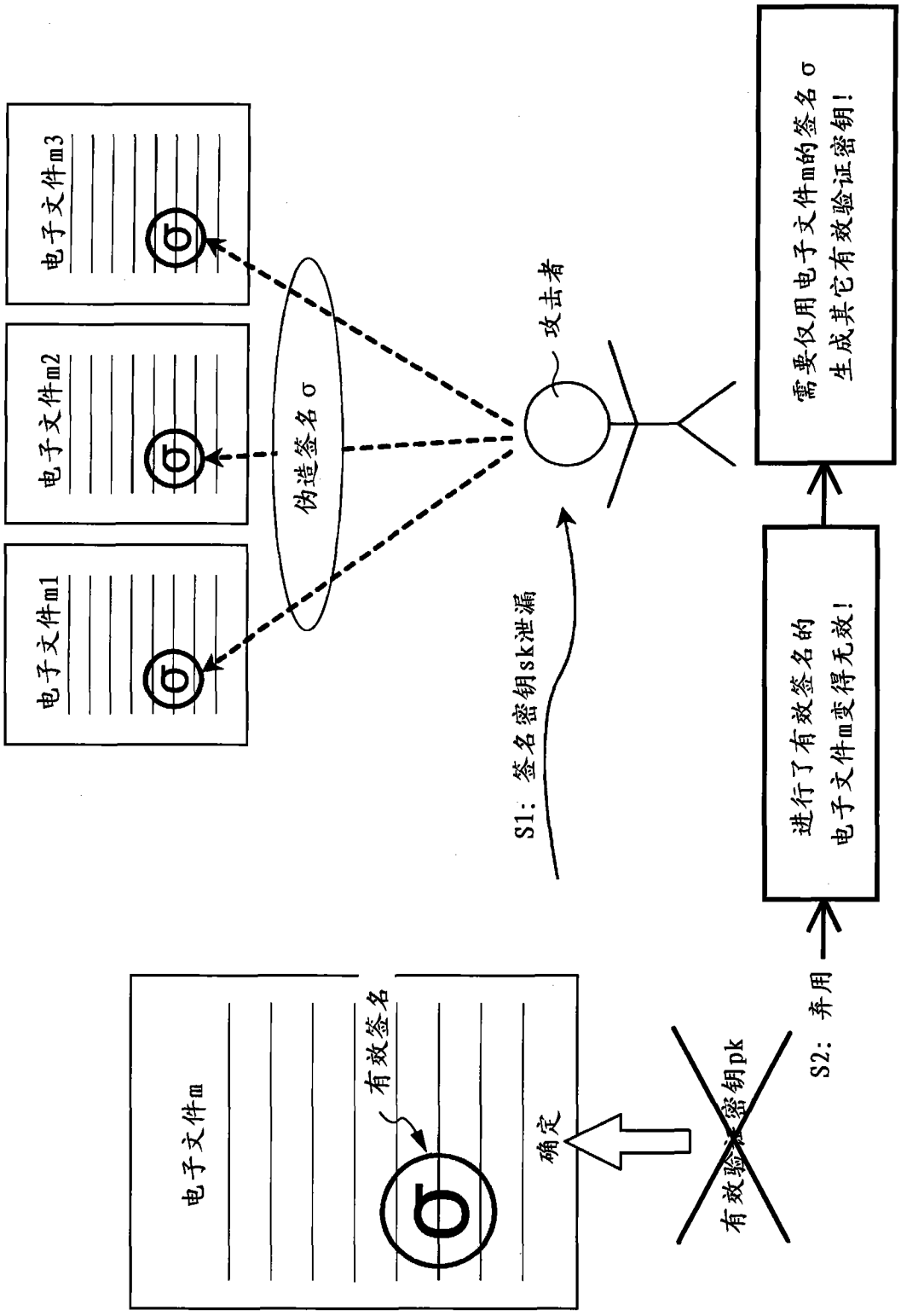

电子文件m3
电子文件m2
电子文件m1
伪造签名 σ
攻击者
需要仅用电子文件m的签名 σ
生成其它有效验证密钥！
S1：签名密钥sk泄漏
进行了有效签名的
电子文件m变得无效！
S2：弃用
电子文件m
有效签名
确定
有效验证密钥pk

图 1

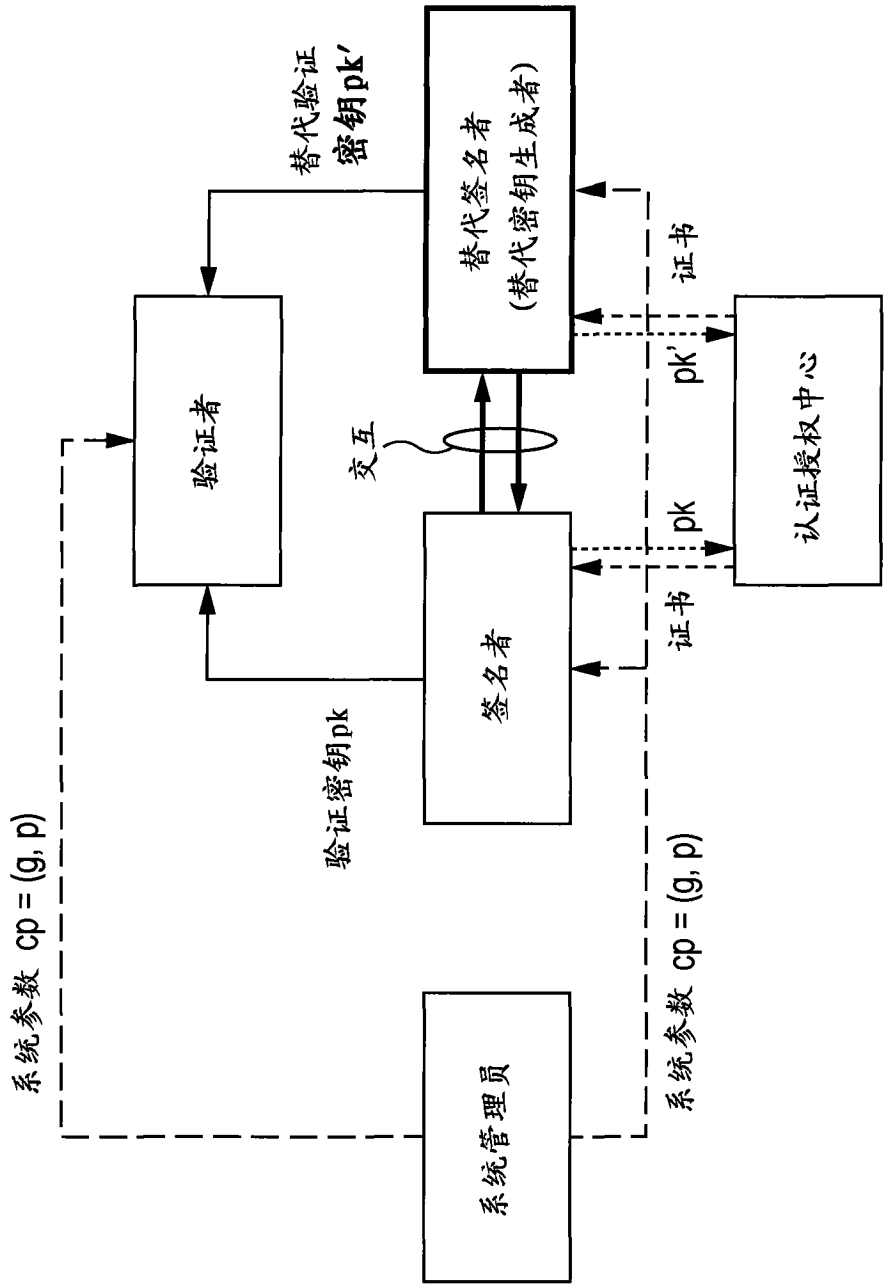

替代验证
密钥pk′
替代签名者
(替代密钥生成者)
验证者
交互
证书
pk′
认证授权中心
pk
证书
签名者
验证密钥pk
系统参数 cp = (g, p)
系统管理员
系统参数 cp = (g, p)

图 2

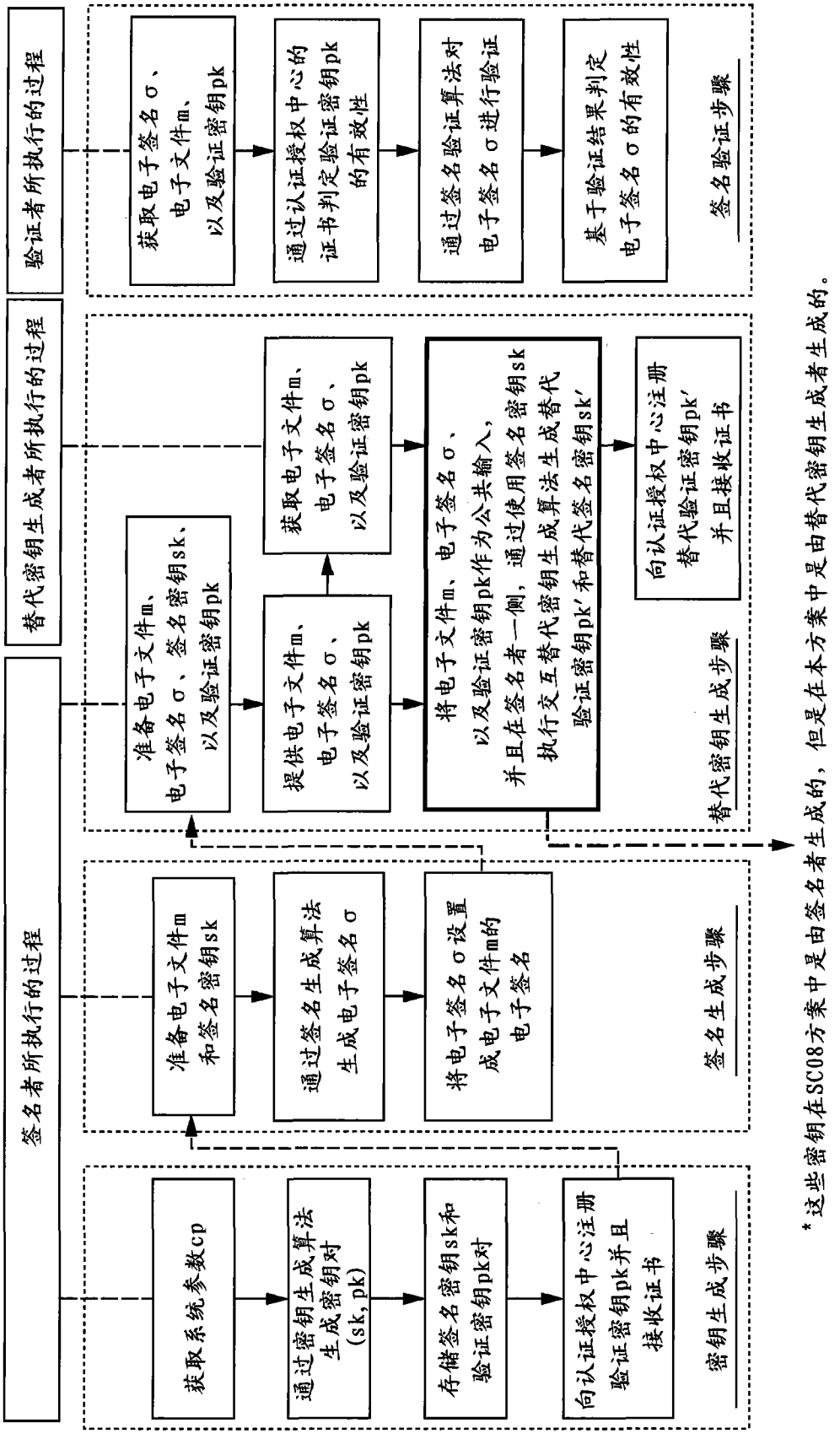
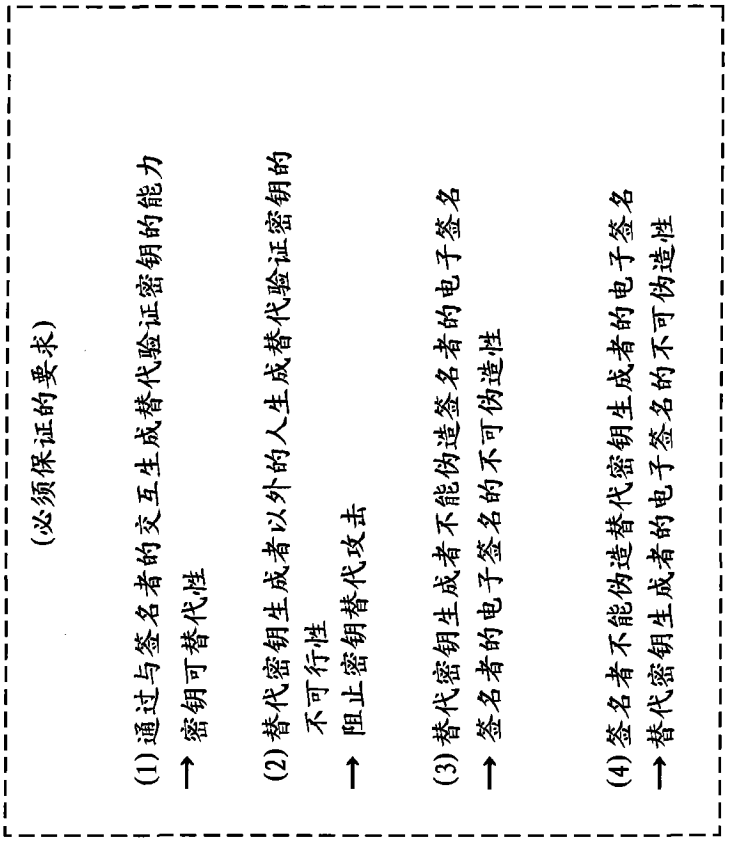

签名者所执行的过程
替代密钥生成者所执行的过程
验证者所执行的过程
获取系统参数cp
通过密钥生成算法生成密钥对(sk,pk)
存储签名密钥sk和验证密钥pk对
向认证授权中心注册验证密钥pk并且接收证书
密钥生成步骤
准备电子文件m和签名密钥sk
通过签名生成算法生成电子签名σ
将电子签名σ设置成电子文件m的电子签名
签名生成步骤
准备电子文件m、电子签名σ、签名密钥sk、以及验证密钥pk
提供电子文件m、电子签名σ、以及验证密钥pk
获取电子文件m、电子签名σ、以及验证密钥pk
将电子文件m、电子签名σ、以及验证密钥pk作为公共输入，并且在签名者一侧，通过使用签名密钥sk执行交互替代密钥生成算法生成替代验证密钥pk′和替代签名密钥sk′
向认证授权中心注册替代验证密钥pk′并且接收证书
替代密钥生成步骤
获取电子签名σ、电子文件m、以及验证密钥pk
通过认证授权中心的证书判定验证密钥pk的有效性
通过签名验证算法对电子签名σ进行验证
基于验证结果判定电子签名σ的有效性
签名验证步骤
*这些密钥在SC08方案中是由签名者生成的，但是在本方案中是由替代密钥生成者生成的。

图 3


(必须保证的要求)
(1) 通过与签名者的交互生成替代验证密钥的能力
→ 密钥可替代性
(2) 替代密钥生成者以外的人生成替代验证密钥的
不可行性
→ 阻止密钥替代攻击
(3) 替代密钥生成者不能伪造签名者的电子签名
→ 签名者的电子签名的不可伪造性
(4) 签名者不能伪造替代密钥生成者的电子签名
→ 替代密钥生成者的电子签名的不可伪造性

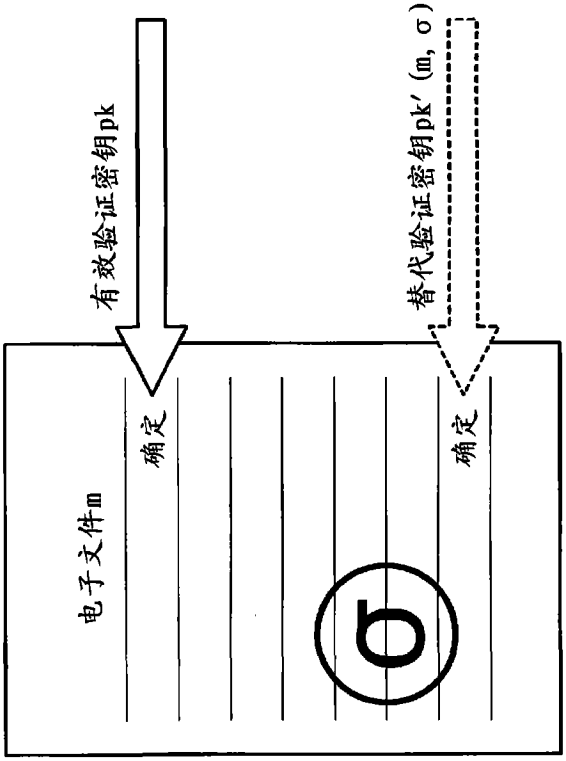

有效验证密钥pk
替代验证密钥pk′(m, σ)
电子文件m
确定
确定
σ

图 4

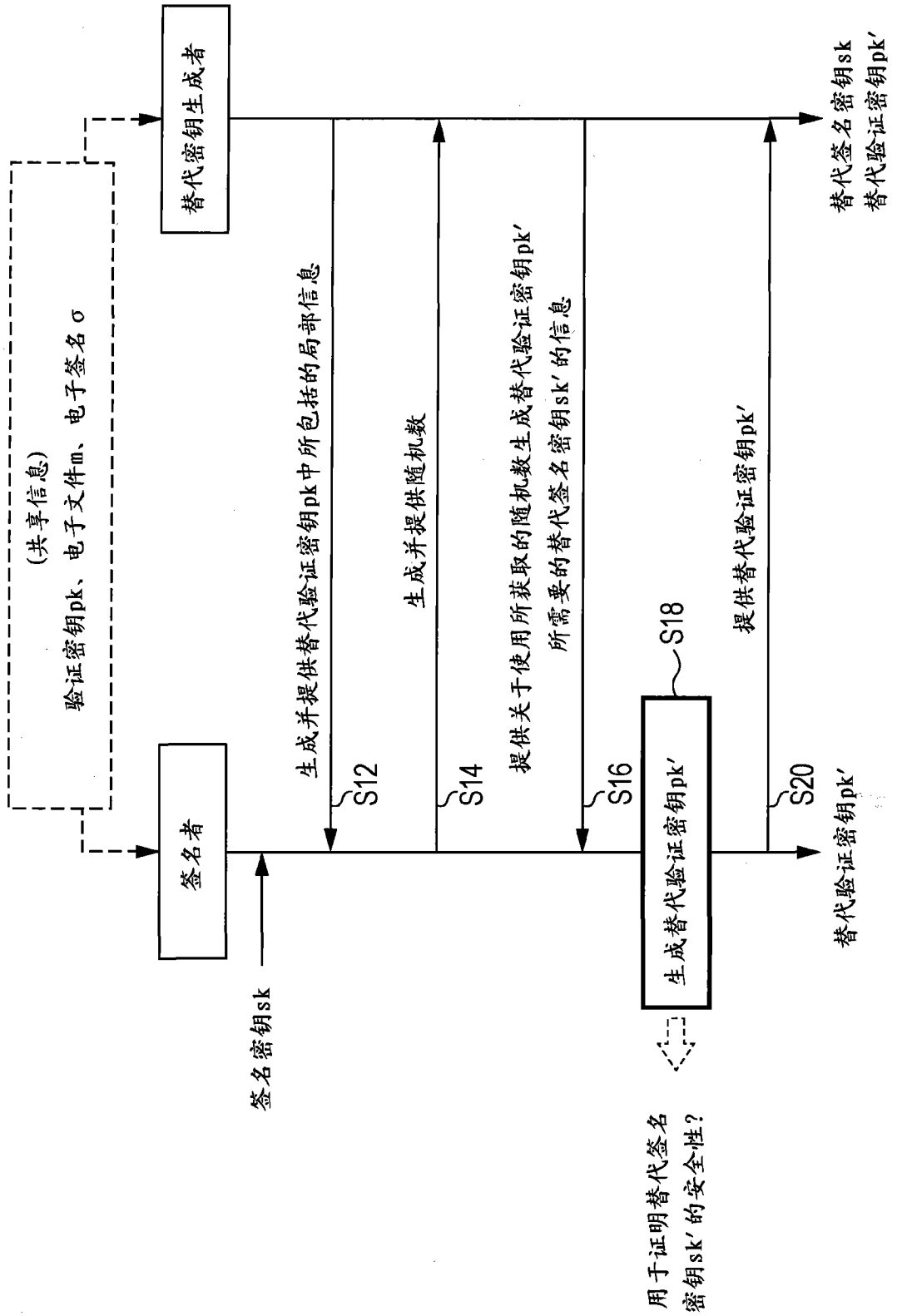

替代密钥生成者
(共享信息)
验证密钥pk、电子文件m、电子签名σ
签名者
签名密钥sk
生成并提供替代验证密钥pk中所包括的局部信息
S12
生成并提供随机数
S14
提供关于使用所获取的随机数生成替代验证密钥pk′
所需要的替代签名密钥sk′的信息
S16
生成替代验证密钥pk′
S18
提供替代验证密钥pk′
S20
替代签名密钥sk
替代验证密钥pk′
用于证明替代签名
密钥sk′的安全性?

图 5

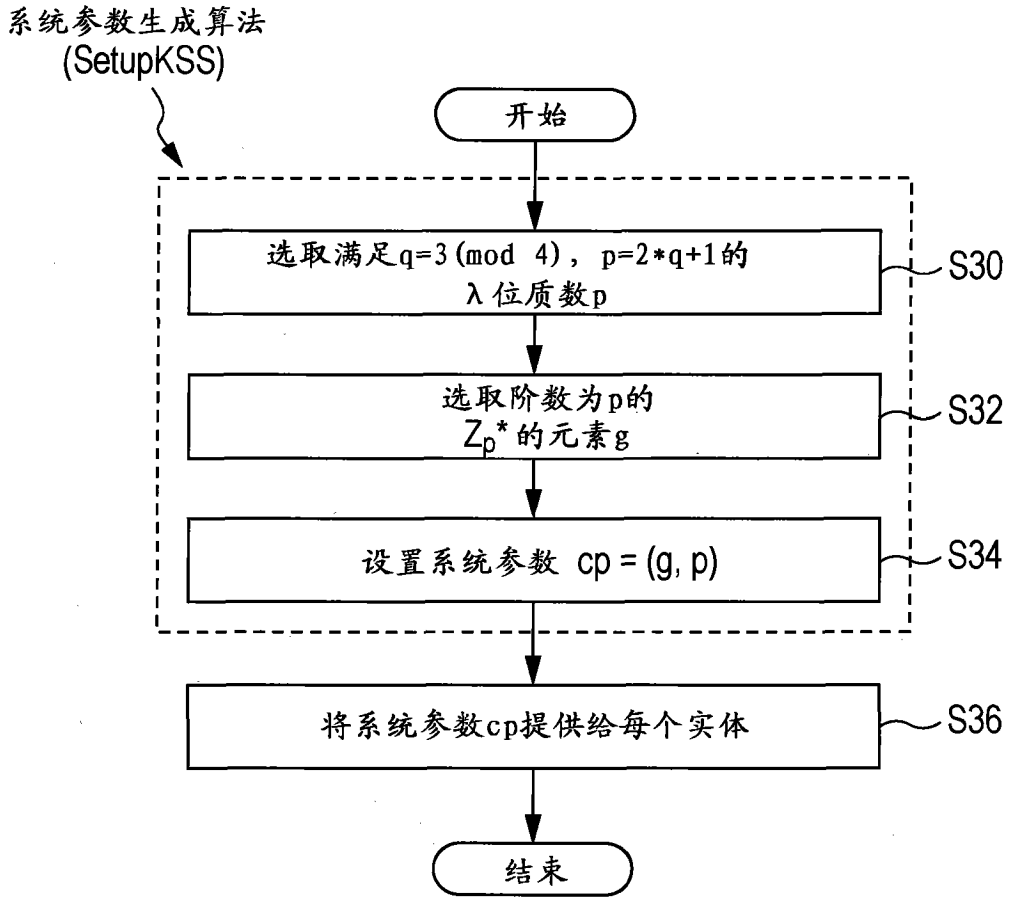

系统参数生成算法
(SetupKSS)
开始
选取满足q=3(mod 4)，p=2*q+1的
λ位质数p
S30
选取阶数为p的
Z_p^*的元素g
S32
设置系统参数 cp = (g, p)
S34
将系统参数cp提供给每个实体
S36
结束

图 6

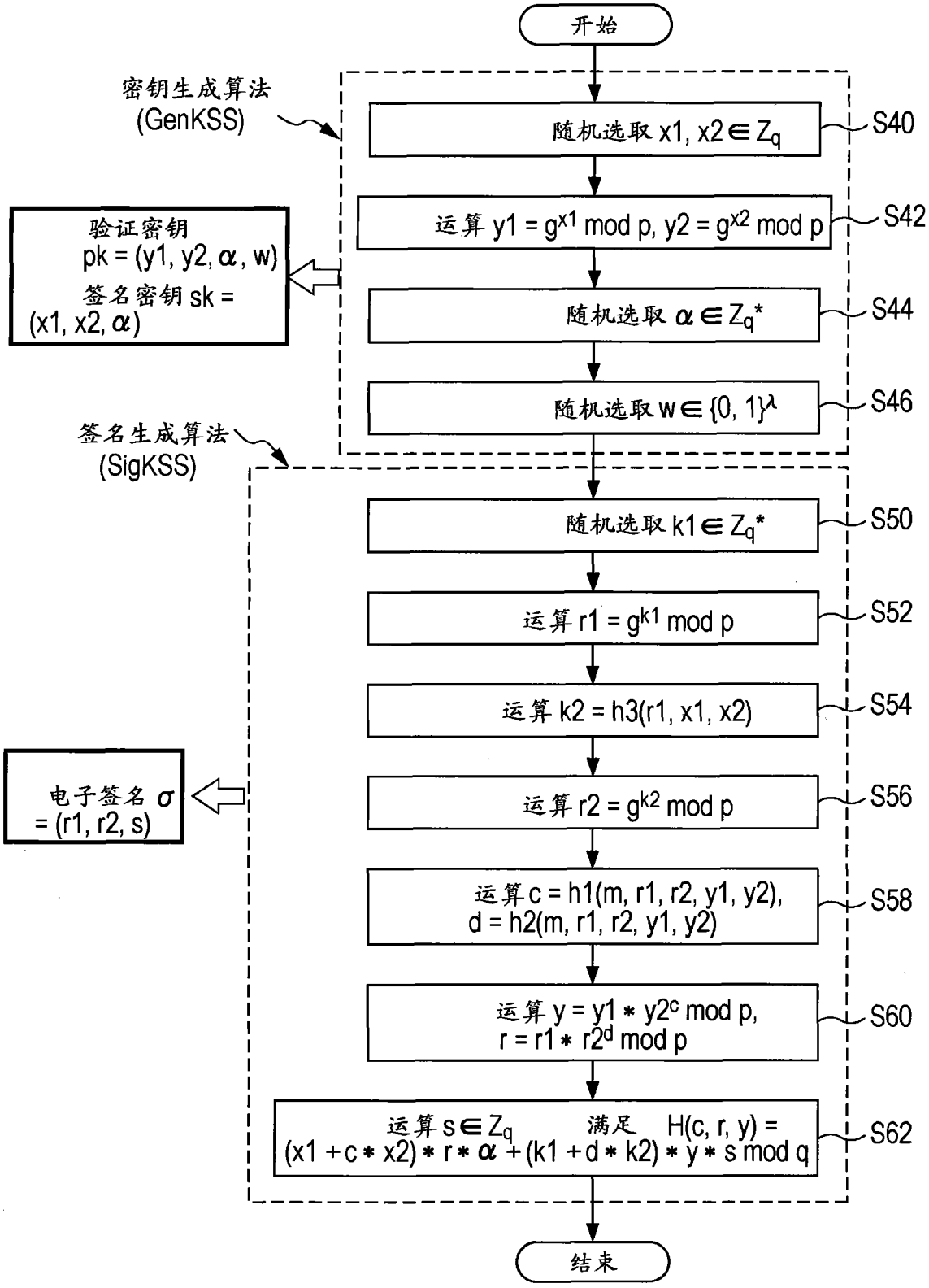

开始
密钥生成算法
(GenKSS)
随机选取 x1, x2∈Zq
S40
运算 y1 = g^x1 mod p, y2 = g^x2 mod p
S42
验证密钥
pk = (y1, y2, α, w)
签名密钥 sk =
(x1, x2, α)
随机选取 α∈Zq*
S44
随机选取 w∈{0, 1}^λ
S46
签名生成算法
(SigKSS)
随机选取 k1∈Zq*
S50
运算 r1 = g^k1 mod p
S52
运算 k2 = h3(r1, x1, x2)
S54
电子签名 σ
= (r1, r2, s)
运算 r2 = g^k2 mod p
S56
运算 c = h1(m, r1, r2, y1, y2),
d = h2(m, r1, r2, y1, y2)
S58
运算 y = y1 * y2^c mod p,
r = r1 * r2^d mod p
S60
运算 s∈Zq 满足 H(c, r, y) =
(x1 + c * x2) * r * α + (k1 + d * k2) * y * s mod q
S62
结束

图 7

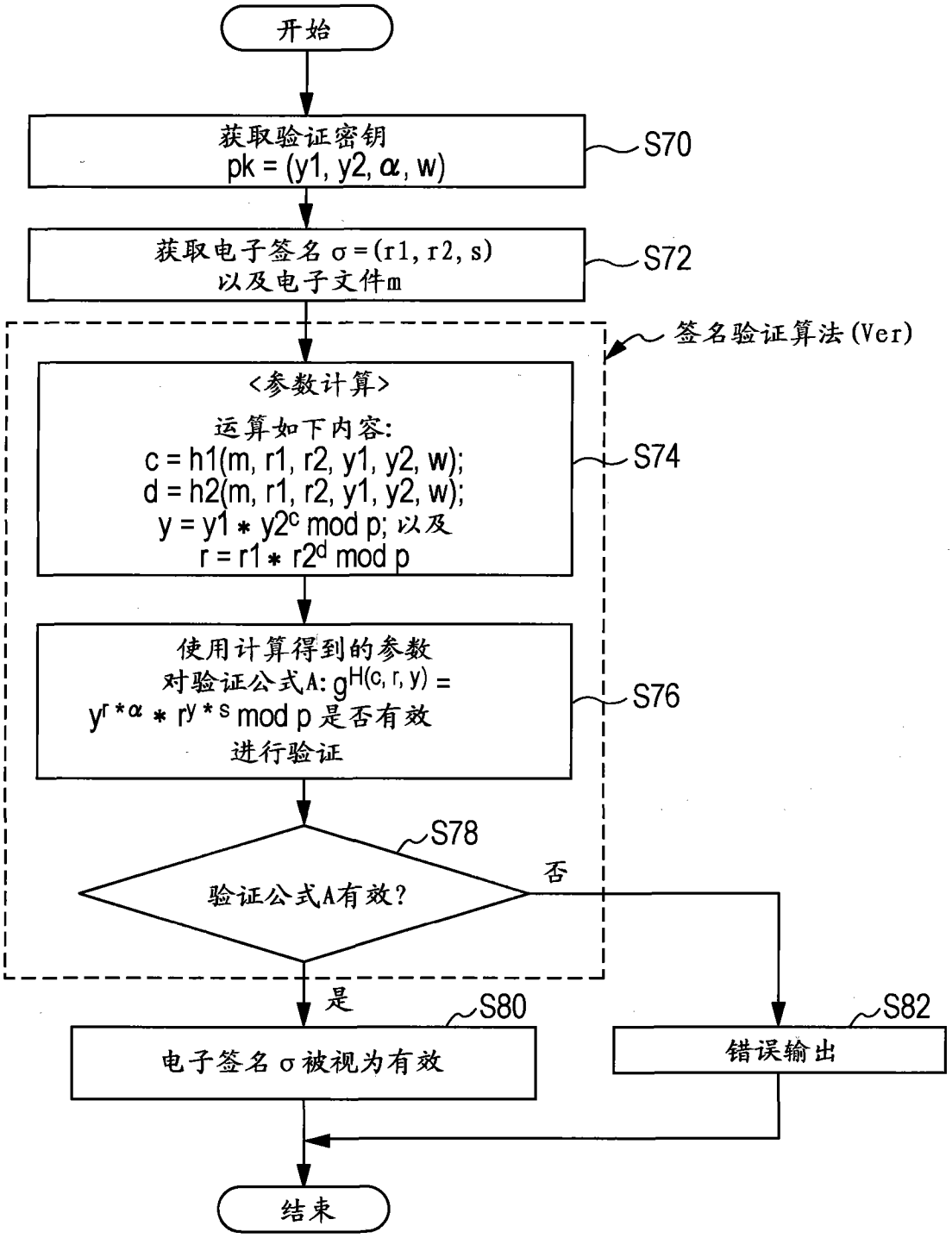

开始
获取验证密钥
pk = (y1, y2, α, w)
S70
获取电子签名 σ = (r1, r2, s)
以及电子文件m
S72
签名验证算法(Ver)
<参数计算>
运算如下内容:
c = h1(m, r1, r2, y1, y2, w);
d = h2(m, r1, r2, y1, y2, w);
y = y1 * y2^c mod p; 以及
r = r1 * r2^d mod p
S74
使用计算得到的参数
对验证公式A: g^H(c, r, y) =
y^r*α * r^y*s mod p 是否有效
进行验证
S76
S78
验证公式A有效?
否
是
S80
电子签名 σ 被视为有效
S82
错误输出
结束

图 8

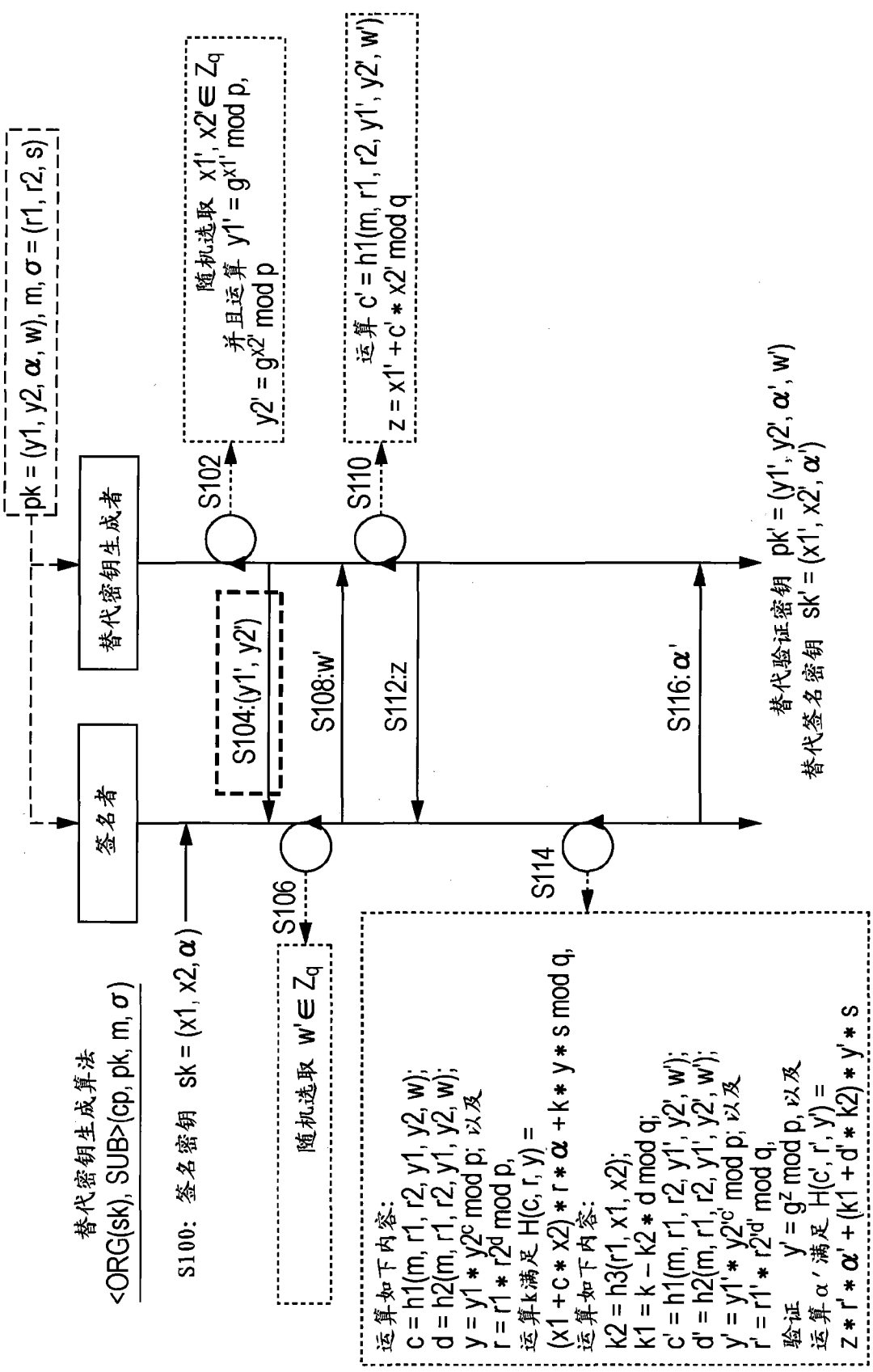

替代密钥生成算法
<ORG(sk), SUB>(cp, pk, m, σ)
S100：签名密钥 sk = (x1, x2, α)
pk = (y1, y2, α, w), m, σ = (r1, r2, s)
签名者
替代密钥生成者
S102
随机选取 x1', x2'∈ Zq
并且运算 y1' = g^x1' mod p,
y2' = g^x2' mod p
S104:(y1', y2')
S106
随机选取 w'∈ Zq
S108:w'
S110
运算 c' = h1(m, r1, r2, y1', y2', w');
z = x1' + c' * x2' mod q
S112:z
S114
运算如下内容:
c = h1(m, r1, r2, y1, y2, w);
d = h2(m, r1, r2, y1, y2, w);
y = y1' * y2^c mod p; 以及
r = r1' * r2^d mod p,
运算k满足 H(c, r, y) =
(x1 + c * x2) * r * α + k * y * s mod q,
运算如下内容:
k2 = h3(r1, x1, x2);
k1 = k – k2 * d mod q;
c' = h1(m, r1, r2, y1', y2', w');
d' = h2(m, r1, r2, y1', y2', w');
y' = y1' * y2'^c' mod p; 以及
r' = r1' * r2'^d' mod q,
验证 y' = g^z mod p, 以及
运算α′满足 H(c', r', y') =
z * r' * α' + (k1 + d' * k2) * y' * s
S116: α'
替代验证密钥 pk' = (y1', y2', α', w')
替代签名密钥 sk' = (x1', x2', α')

图 9

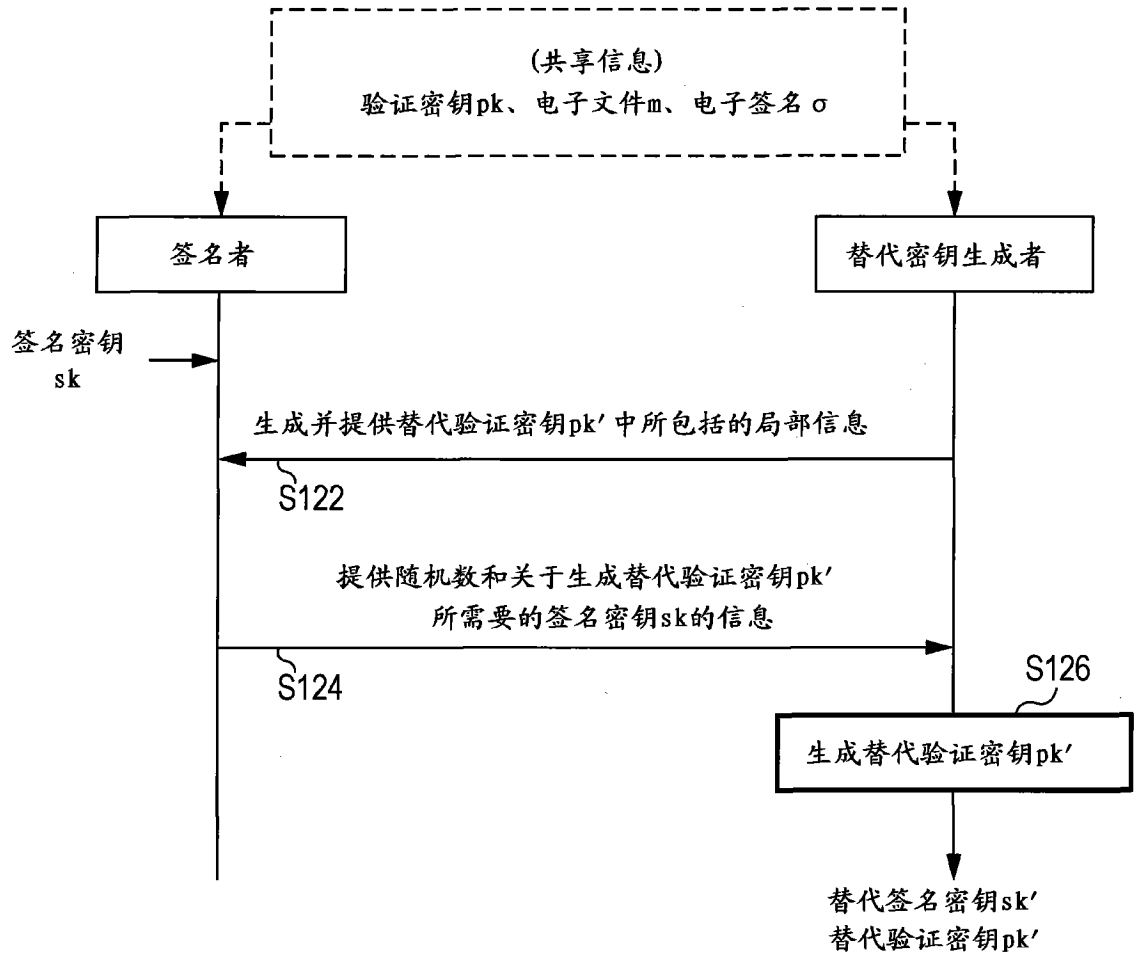

(共享信息)
验证密钥pk、电子文件m、电子签名σ
签名者
替代密钥生成者
签名密钥
sk
生成并提供替代验证密钥pk′中所包括的局部信息
S122
提供随机数和关于生成替代验证密钥pk′
所需要的签名密钥sk的信息
S124
S126
生成替代验证密钥pk′
替代签名密钥sk′
替代验证密钥pk′

图 10

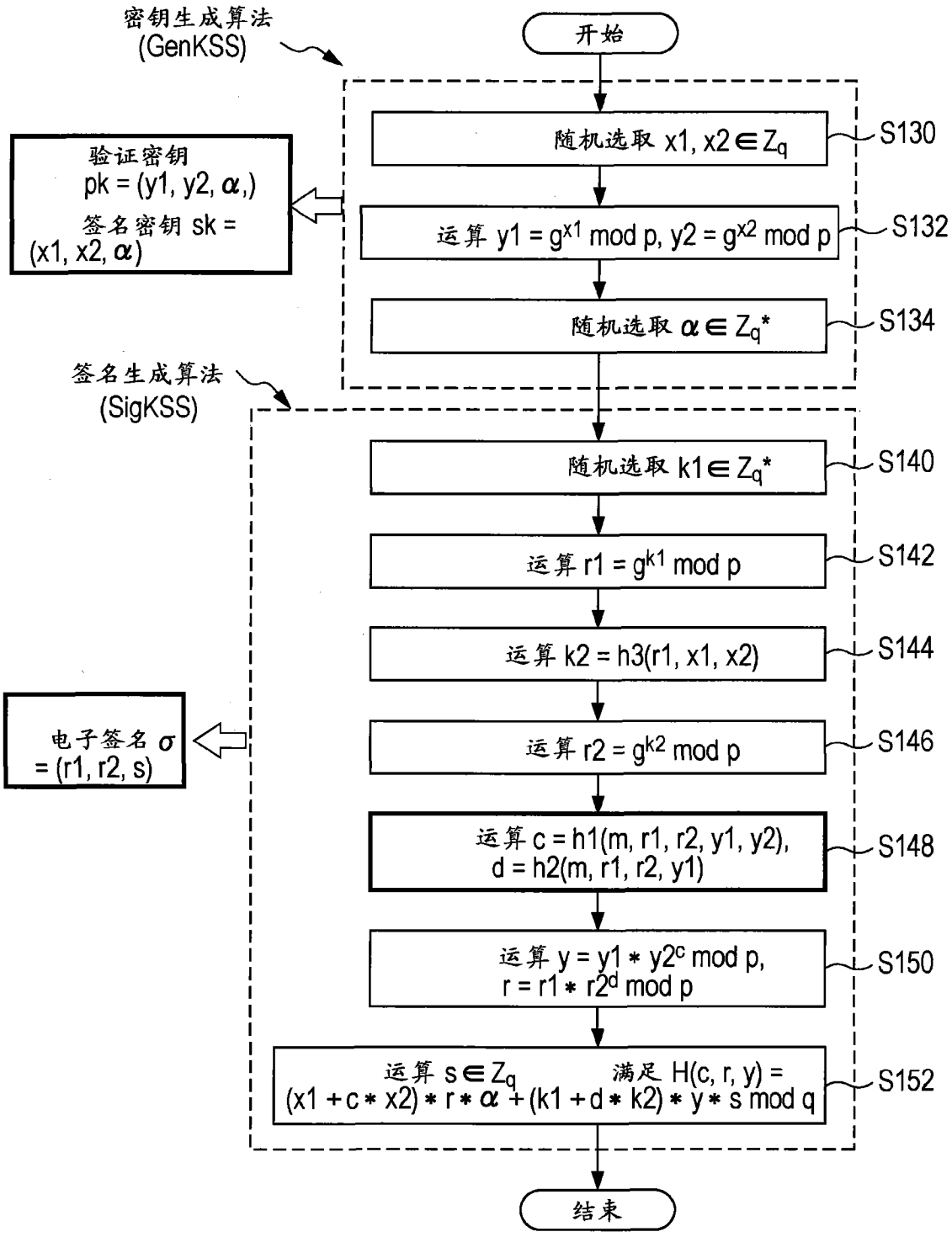

密钥生成算法
(GenKSS)
开始
随机选取 x1, x2∈Zq
S130
验证密钥
pk = (y1, y2, α,)
签名密钥 sk =
(x1, x2, α)
运算 y1 = g^x1 mod p, y2 = g^x2 mod p
S132
随机选取 α∈Zq*
S134
签名生成算法
(SigKSS)
随机选取 k1∈Zq*
S140
运算 r1 = g^k1 mod p
S142
运算 k2 = h3(r1, x1, x2)
S144
电子签名 σ
= (r1, r2, s)
运算 r2 = g^k2 mod p
S146
运算 c = h1(m, r1, r2, y1, y2),
d = h2(m, r1, r2, y1)
S148
运算 y = y1 * y2^c mod p,
r = r1 * r2^d mod p
S150
运算 s∈Zq 满足 H(c, r, y) =
(x1 + c * x2) * r * α + (k1 + d * k2) * y * s mod q
S152
结束

图 11

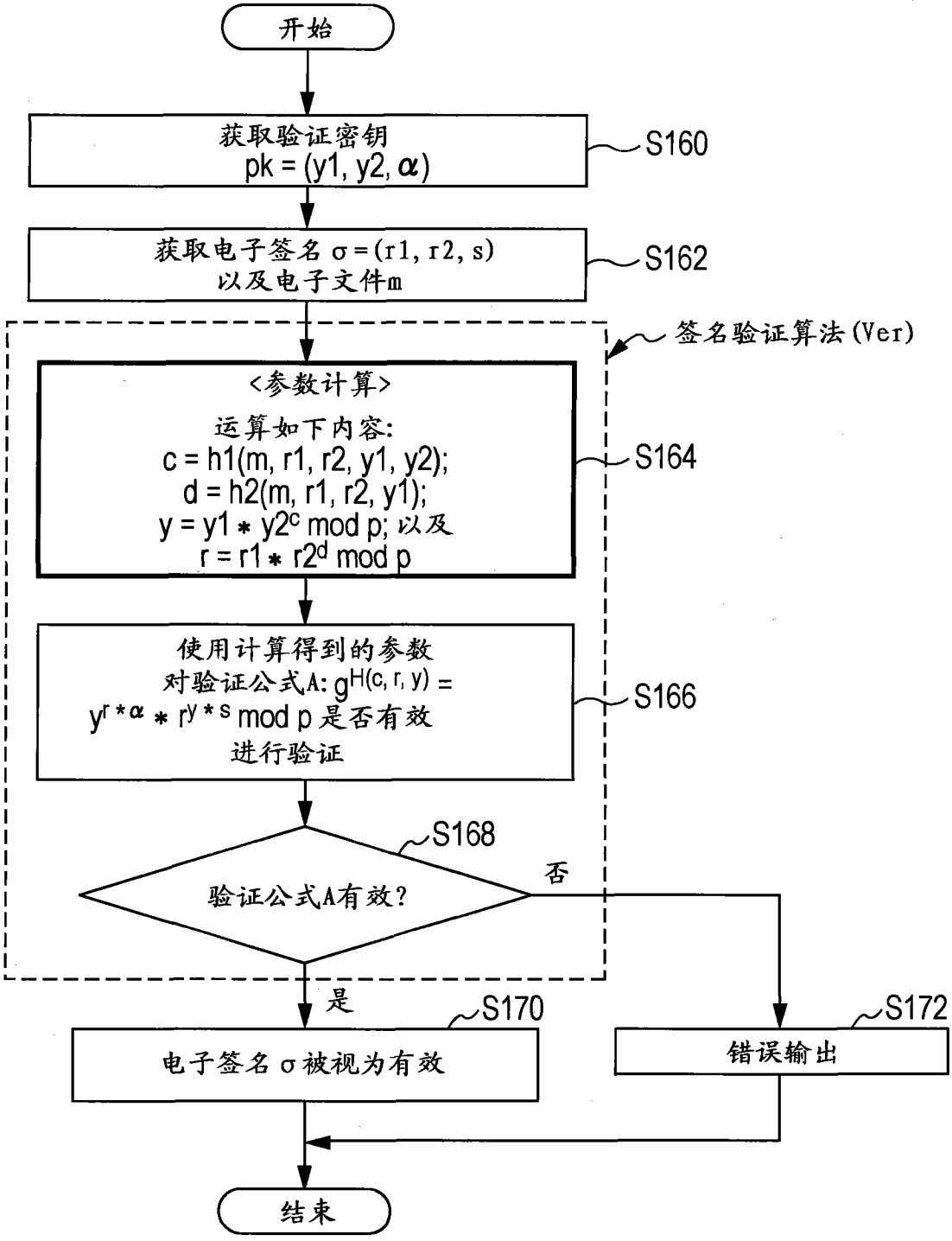

开始
获取验证密钥
pk = (y1, y2, α)
S160
获取电子签名 σ = (r1, r2, s)
以及电子文件m
S162
签名验证算法(Ver)
<参数计算>
运算如下内容:
c = h1(m, r1, r2, y1, y2);
d = h2(m, r1, r2, y1);
y = y1 * y2^c mod p; 以及
r = r1 * r2^d mod p
S164
使用计算得到的参数
对验证公式A: g^H(c, r, y) =
y^r*α * r^y*s mod p 是否有效
进行验证
S166
S168
验证公式A有效?
否
是
S170
电子签名 σ 被视为有效
S172
错误输出
结束

图 12

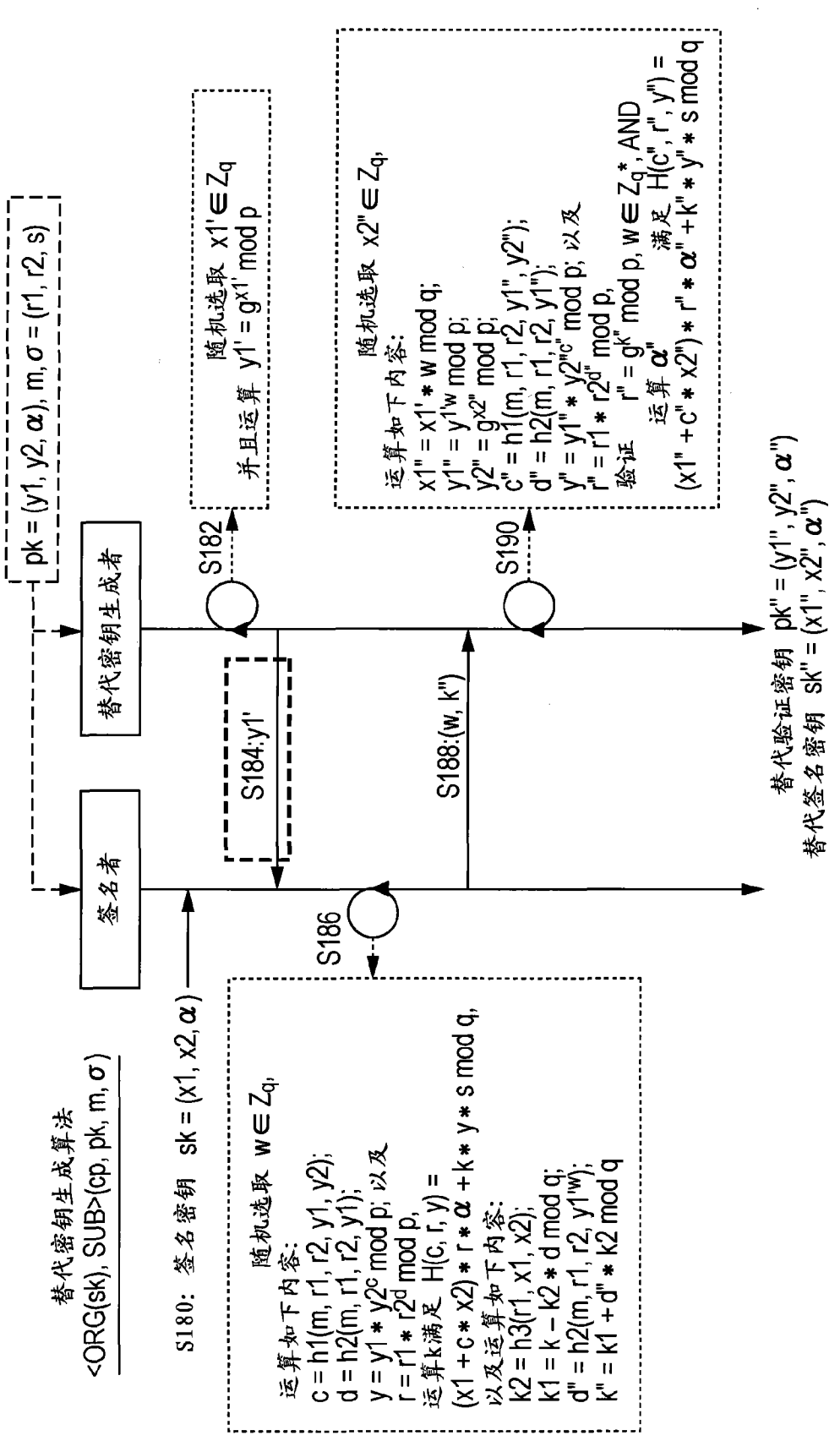

替代密钥生成算法
<ORG(sk), SUB>(cp, pk, m, σ)
S180: 签名密钥 sk = (x1, x2, α)
pk = (y1, y2, α), m, σ = (r1, r2, s)
签名者
替代密钥生成者
S182
随机选取 x1'∈Zq
并且运算 y1' = g^x1' mod p
S184:y1'
S186
随机选取 w∈Zq,
运算如下内容:
c = h1(m, r1, r2, y1, y2);
d = h2(m, r1, r2, y1);
y = y1 * y2^c mod p; 以及
r = r1 * r2^d mod p,
运算k,满足 H(c, r, y) =
(x1 + c * x2) * r * α + k * y * s mod q,
以及运算如下内容:
k2 = h3(r1, x1, x2);
k1 = k – k2 * d mod q;
d'' = h2(m, r1, r2, y1^w);
k'' = k1 + d'' * k2 mod q
S188:(w, k'')
S190
随机选取 x2''∈Zq,
运算如下内容:
x1'' = x1' * w mod q;
y1'' = y1^w mod p;
y2'' = g^x2'' mod p;
c'' = h1(m, r1, r2, y1'', y2'');
d'' = h2(m, r1, r2, y1'');
y'' = y1'' * y2''^c'' mod p; 以及
r'' = r1 * r2^d'' mod p,
验证 r'' = g^k'' mod p, w∈Zq*, AND
运算 α'' 满足 H(c'', r'', y'') =
(x1'' + c'' * x2'') * r'' * α'' + k'' * y'' * s mod q
替代验证密钥 pk'' = (y1'', y2'', α'')
替代签名密钥 sk'' = (x1'', x2'', α'')

图 13

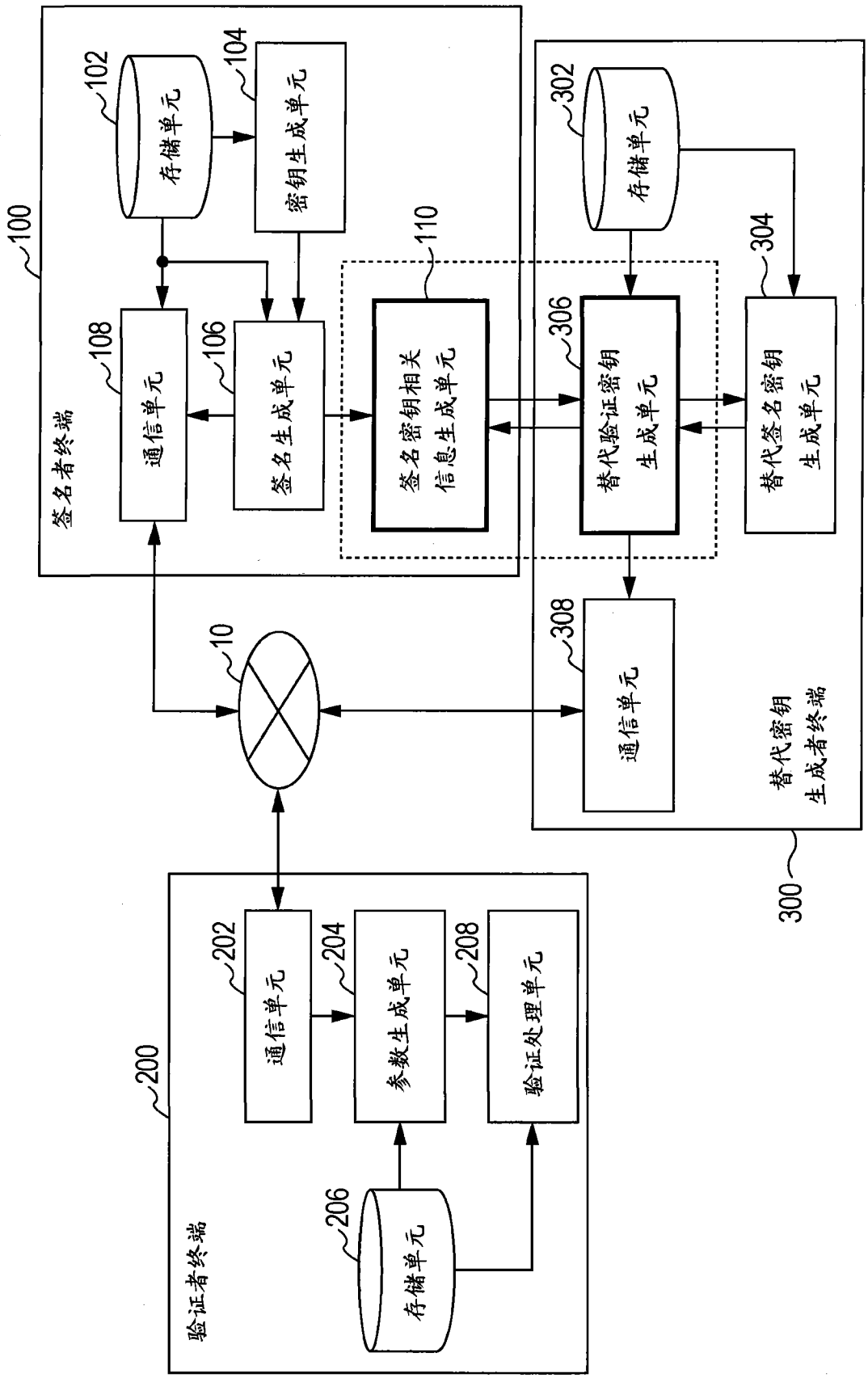

100
签名者终端
102
存储单元
104
密钥生成单元
108
通信单元
106
签名生成单元
110
签名密钥相关信息生成单元
10
300
替代密钥生成者终端
302
存储单元
304
替代签名密钥生成单元
306
替代验证密钥生成单元
308
通信单元
200
验证者终端
202
通信单元
204
参数生成单元
208
验证处理单元
206
存储单元

图 14

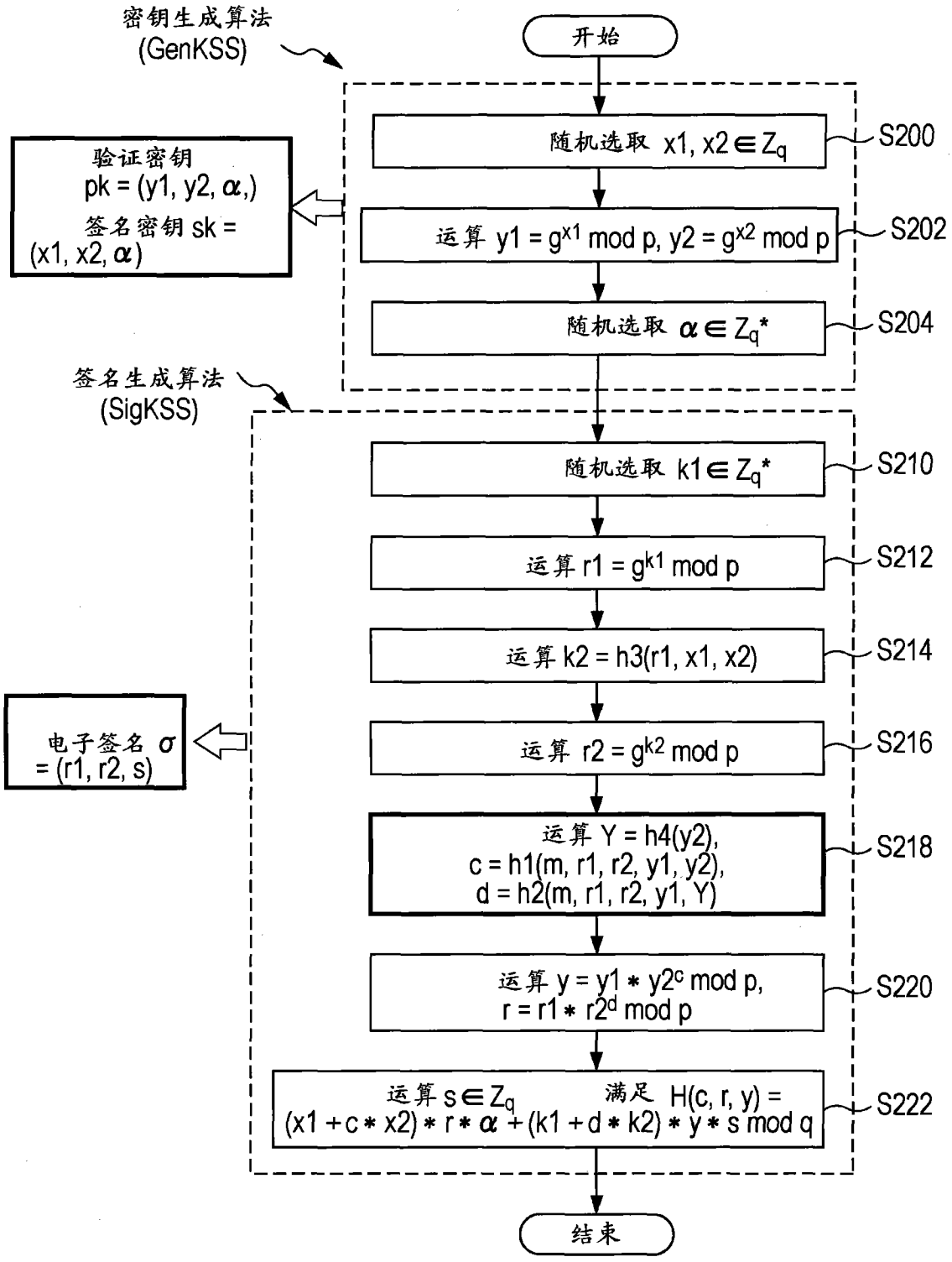

密钥生成算法
(GenKSS)
开始
随机选取 x1, x2∈Zq
S200
验证密钥
pk = (y1, y2, α,)
签名密钥 sk =
(x1, x2, α)
运算 y1 = g^x1 mod p, y2 = g^x2 mod p
S202
随机选取 α∈Zq*
S204
签名生成算法
(SigKSS)
随机选取 k1∈Zq*
S210
运算 r1 = g^k1 mod p
S212
运算 k2 = h3(r1, x1, x2)
S214
电子签名 σ
= (r1, r2, s)
运算 r2 = g^k2 mod p
S216
运算 Y = h4(y2),
c = h1(m, r1, r2, y1, y2),
d = h2(m, r1, r2, y1, Y)
S218
运算 y = y1 * y2^c mod p,
r = r1 * r2^d mod p
S220
运算 s∈Zq 满足 H(c, r, y) =
(x1 + c * x2) * r * α + (k1 + d * k2) * y * s mod q
S222
结束

图 15

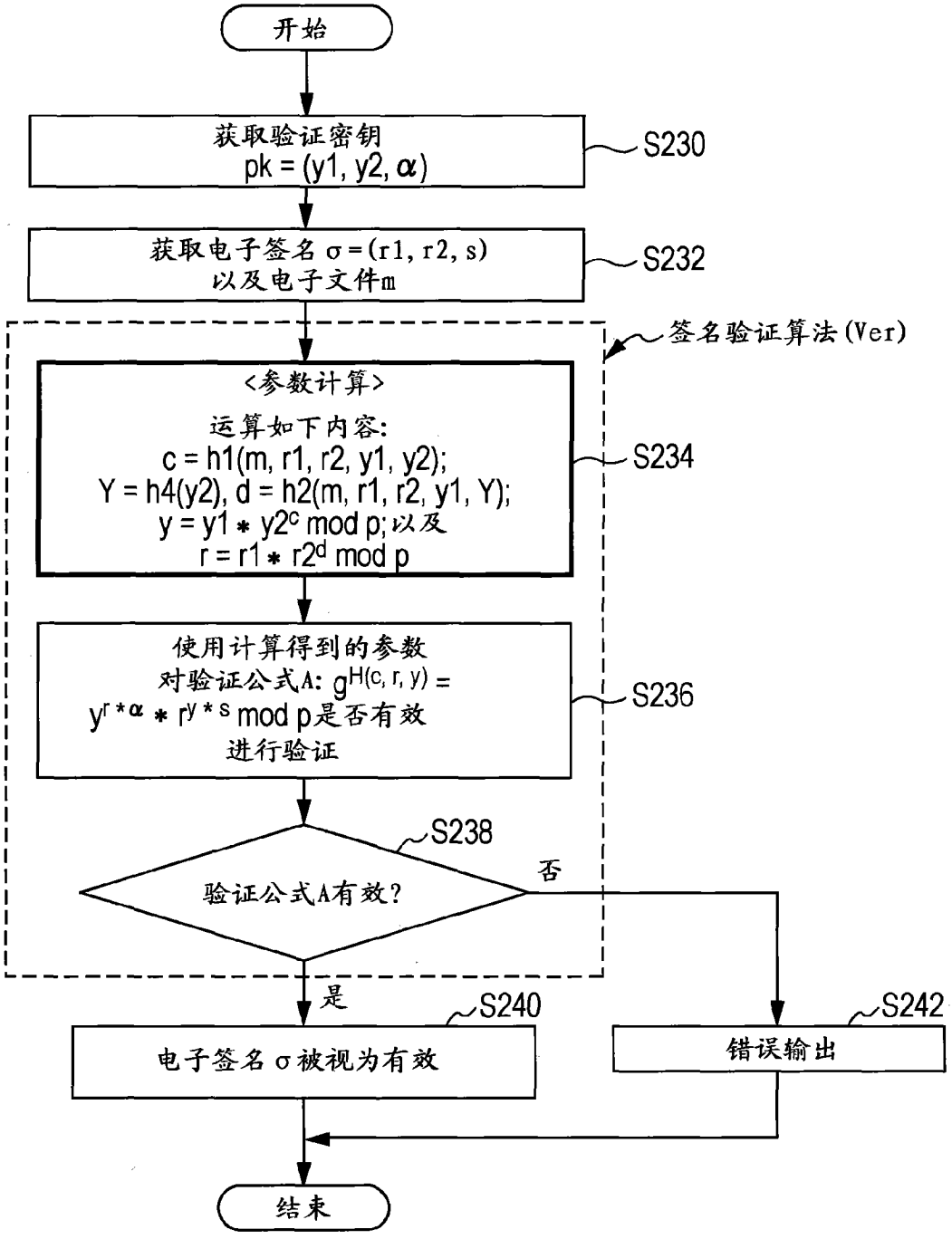

开始
获取验证密钥
pk = (y1, y2, α)
S230
获取电子签名 σ=(r1, r2, s)
以及电子文件m
S232
签名验证算法(Ver)
<参数计算>
运算如下内容:
c = h1(m, r1, r2, y1, y2);
Y = h4(y2), d = h2(m, r1, r2, y1, Y);
y = y1 * y2^c mod p;以及
r = r1 * r2^d mod p
S234
使用计算得到的参数
对验证公式A: g^H(c, r, y) =
y^r*α * r^y*s mod p是否有效
进行验证
S236
S238
验证公式A有效?
否
是
S240
电子签名 σ被视为有效
S242
错误输出
结束

图 16

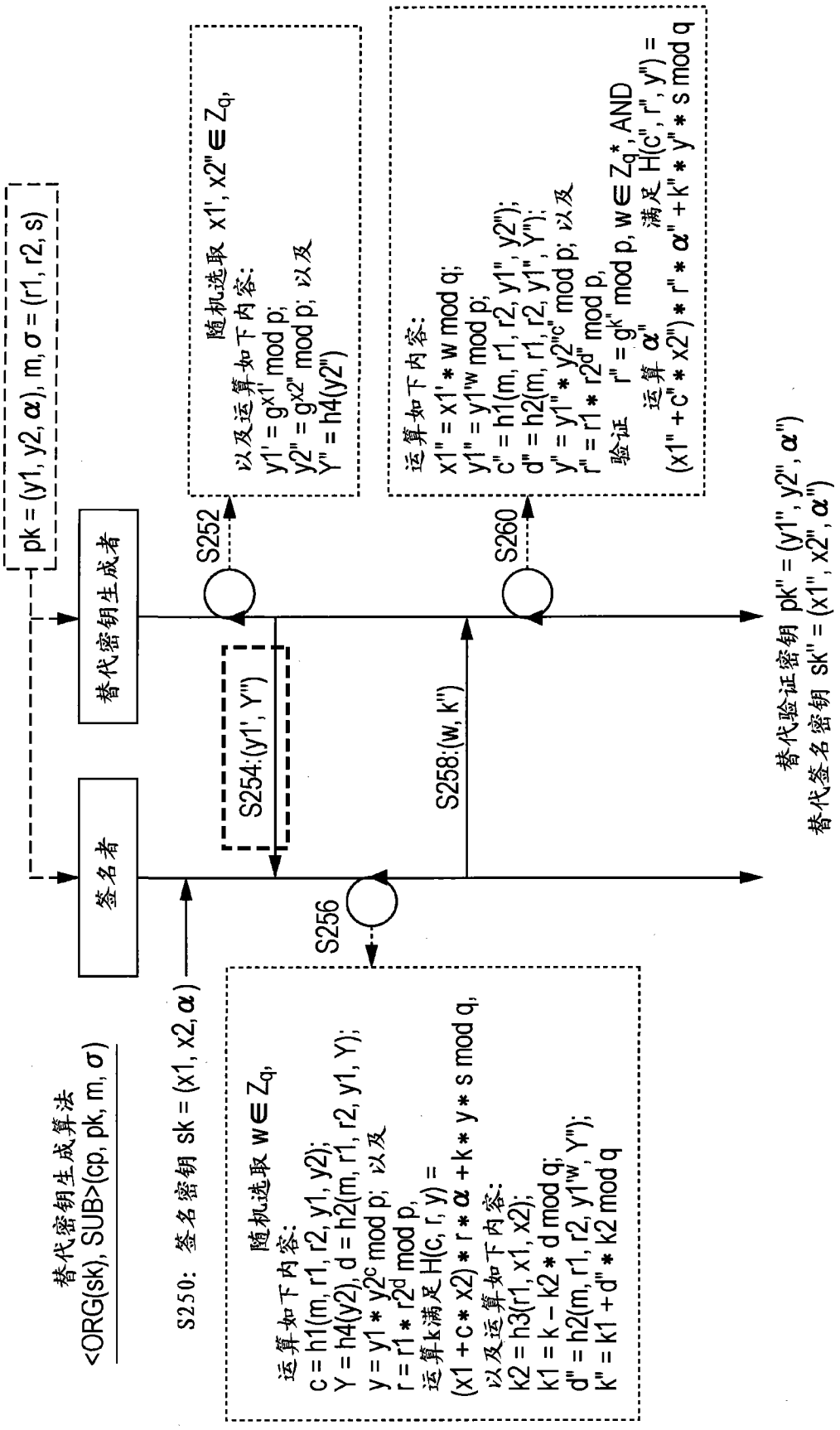

替代密钥生成算法
<ORG(sk), SUB>(cp, pk, m, σ)
pk = (y1, y2, α), m, σ = (r1, r2, s)
签名者
替代密钥生成者
S250: 签名密钥 sk = (x1, x2, α)
随机选取 w∈Zq,
运算如下内容:
c = h1(m, r1, r2, y1, y2);
Y = h4(y2), d = h2(m, r1, r2, y1, Y);
y = y1 * y2^c mod p; 以及
r = r1 * r2^d mod p,
运算k满足 H(c, r, y) =
(x1 + c * x2) * r * α + k * y * s mod q,
以及运算如下内容:
k2 = h3(r1, x1, x2);
k1 = k – k2 * d mod q;
d" = h2(m, r1, r2, y1", Y");
k" = k1 + d" * k2 mod q
S252
随机选取 x1', x2"∈Zq,
以及运算如下内容:
y1' = g^x1' mod p;
y2" = g^x2" mod p; 以及
Y" = h4(y2")
S254:(y1', Y")
S256
S258:(w, k")
S260
运算如下内容:
x1" = x1' * w mod q;
y1" = y1'^w mod p;
c" = h1(m, r1, r2, y1", y2");
d" = h2(m, r1, r2, y1", Y");
y" = y1" * y2"^c" mod p; 以及
r" = r1 * r2^d" mod p,
验证 r" = g^k" mod p, w∈Zq*, AND
运算 α" 满足 H(c", r", y") =
(x1" + c" * x2") * r" * α" + k" * y" * s mod q
替代验证密钥 pk" = (y1", y2", α")
替代签名密钥 sk" = (x1", x2", α")

图 17

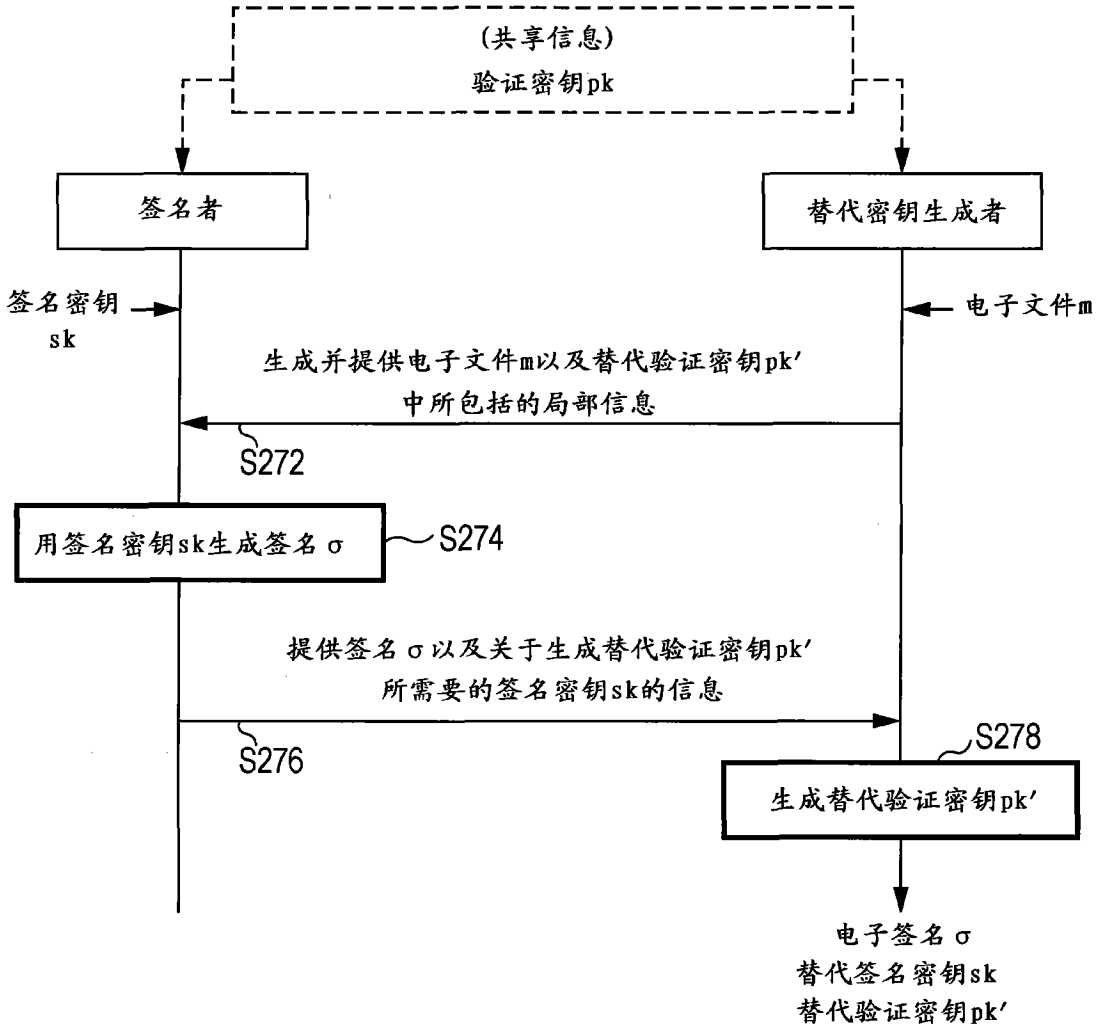

(共享信息)
验证密钥pk
签名者
替代密钥生成者
签名密钥
sk
电子文件m
生成并提供电子文件m以及替代验证密钥pk′
中所包括的局部信息
S272
用签名密钥sk生成签名 σ
S274
提供签名 σ 以及关于生成替代验证密钥pk′
所需要的签名密钥sk的信息
S276
S278
生成替代验证密钥pk′
电子签名 σ
替代签名密钥sk
替代验证密钥pk′

图 18

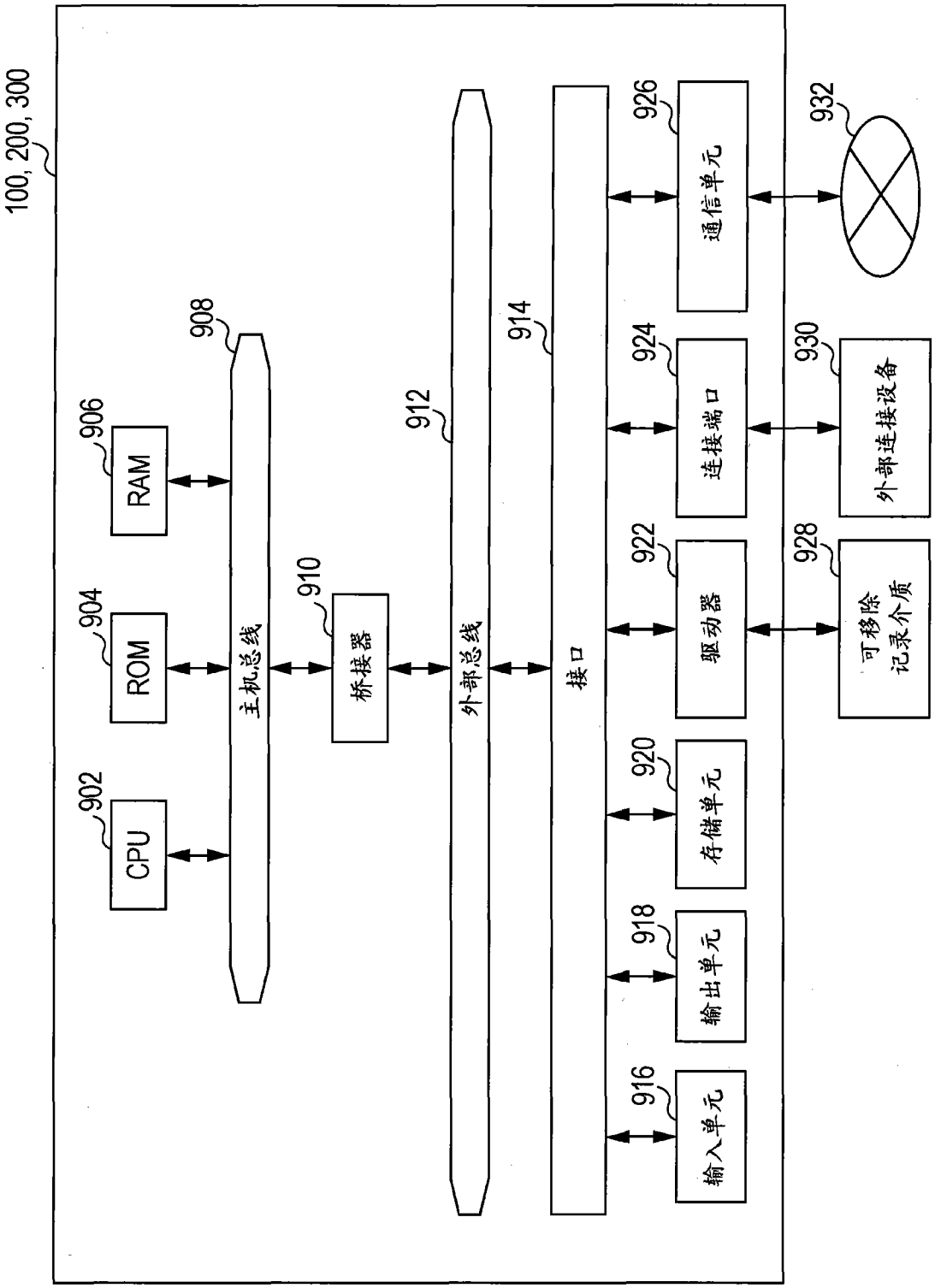
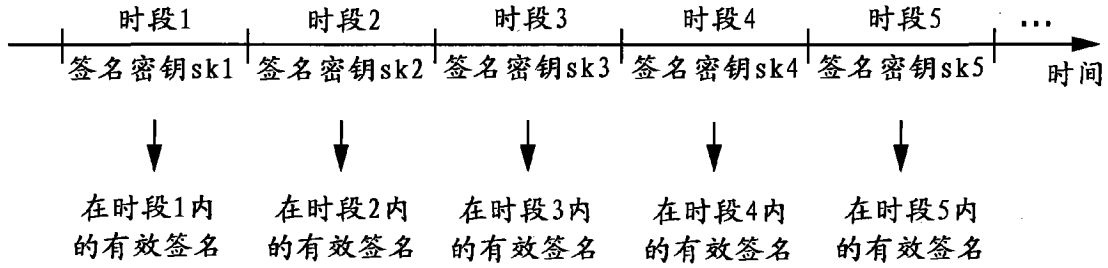
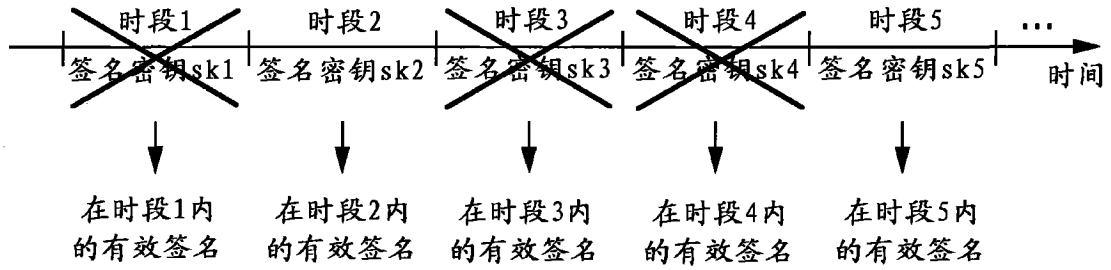

100, 200, 300
902
CPU
904
ROM
906
RAM
908
主机总线
910
桥接器
912
外部总线
914
接口
916
输入单元
918
输出单元
920
存储单元
922
驱动器
924
连接端口
926
通信单元
928
可移除记录介质
930
外部连接设备
932

图 19

(A: 无泄漏)



(B: 有泄漏)



(C: 无效签名)

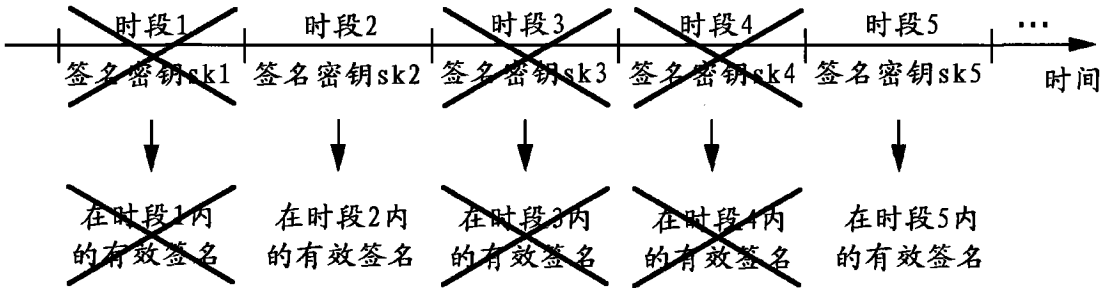


图 20

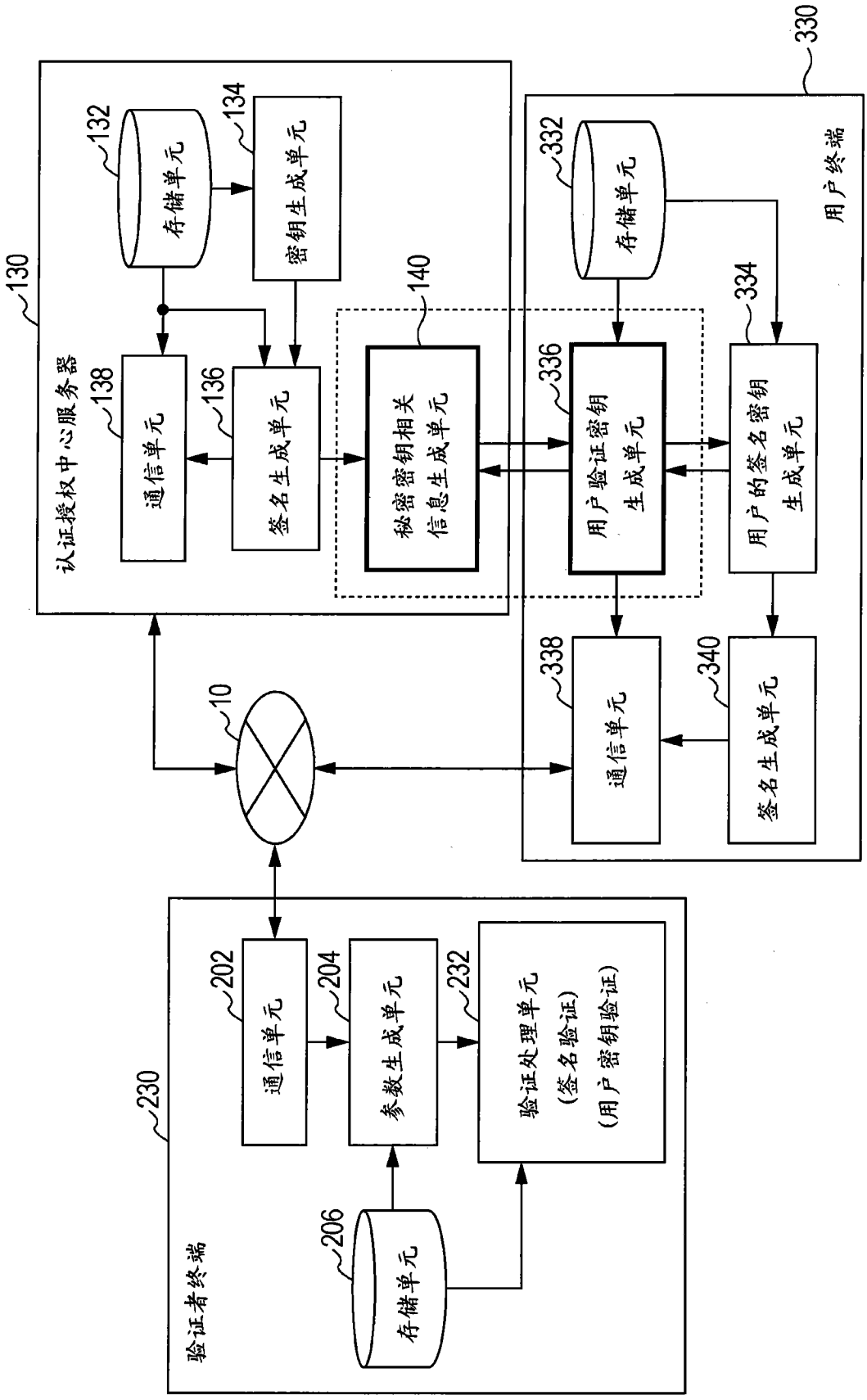

130
认证授权中心服务器
132
存储单元
134
密钥生成单元
138
通信单元
136
签名生成单元
140
秘密密钥相关信息生成单元
330
用户终端
332
存储单元
334
用户的签名密钥生成单元
336
用户验证密钥生成单元
338
通信单元
340
签名生成单元
10
230
验证者终端
202
通信单元
204
参数生成单元
232
验证处理单元
(签名验证)
(用户密钥验证)
206
存储单元

图 21

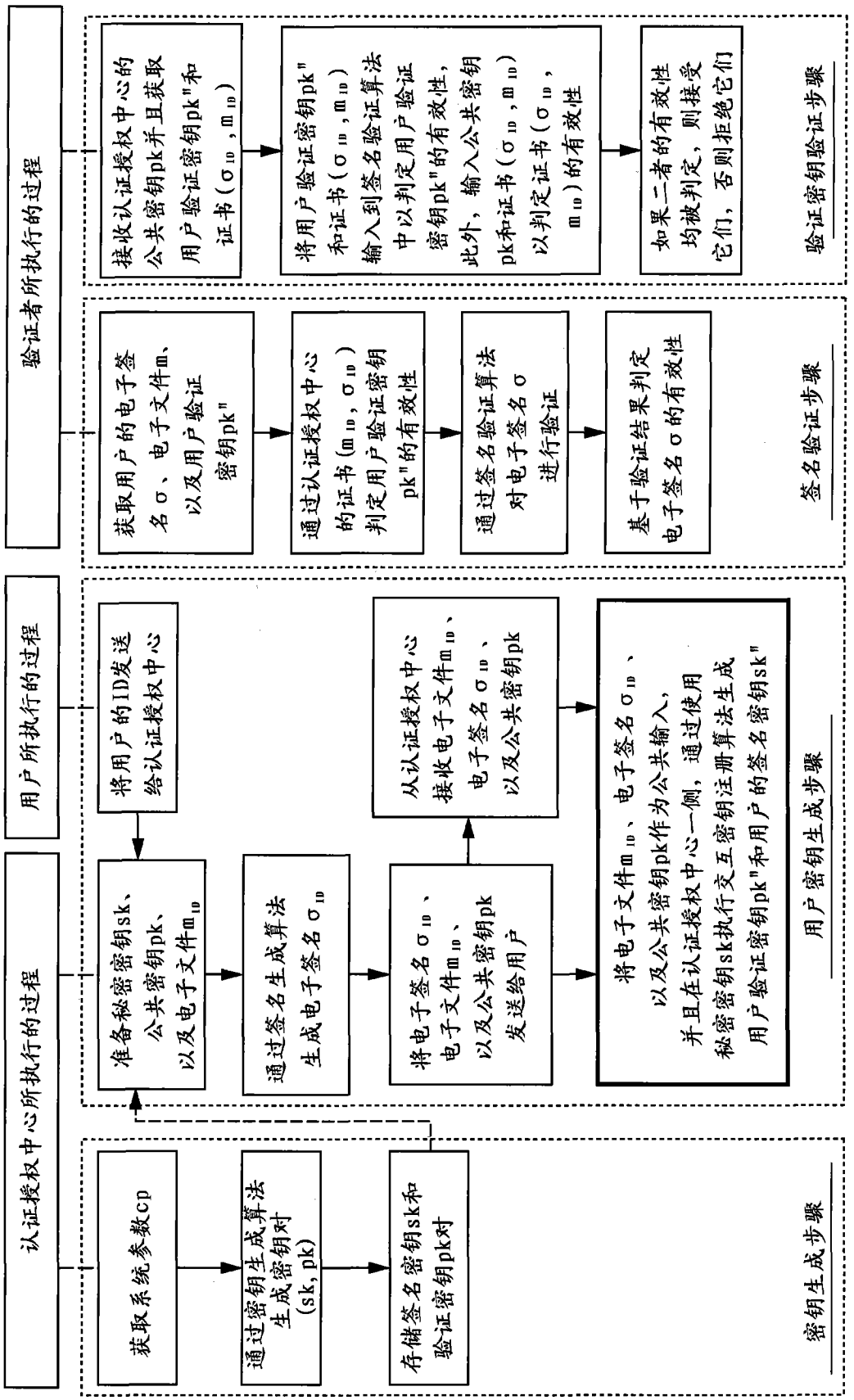

认证授权中心所执行的过程
用户所执行的过程
验证者所执行的过程
获取系统参数cp
通过密钥生成算法生成密钥对(sk, pk)
存储签名密钥sk和验证密钥pk对
密钥生成步骤
将用户的ID发送给认证授权中心
准备秘密密钥sk、公共密钥pk、以及电子文件m ID
通过签名生成算法生成电子签名σ ID
将电子签名σ ID、电子文件m ID、以及公共密钥pk发送给用户
从认证授权中心接收电子文件m ID、电子签名σ ID、以及公共密钥pk
将电子文件m ID、电子签名σ ID、以及公共密钥pk作为公共输入，并且在认证授权中心一侧，通过使用秘密密钥sk执行交互密钥注册算法生成用户验证密钥pk"和用户的签名密钥sk"
用户密钥生成步骤
获取用户的电子签名σ、电子文件m、以及用户验证密钥pk"
通过认证授权中心的证书(m ID, σ ID)判定用户验证密钥pk"的有效性
通过签名验证算法对电子签名σ进行验证
基于验证结果判定电子签名σ的有效性
签名验证步骤
接收认证授权中心的公共密钥pk并且获取用户验证密钥pk"和证书(σ ID, m ID)
将用户验证密钥pk"和证书(σ ID, m ID)输入到签名验证算法中以判定用户验证密钥pk"的有效性，此外，输入公共密钥pk和证书(σ ID, m ID)以判定证书(σ ID, m ID)的有效性
如果二者的有效性均被判定，则接受它们，否则拒绝它们
验证密钥验证步骤

图 22

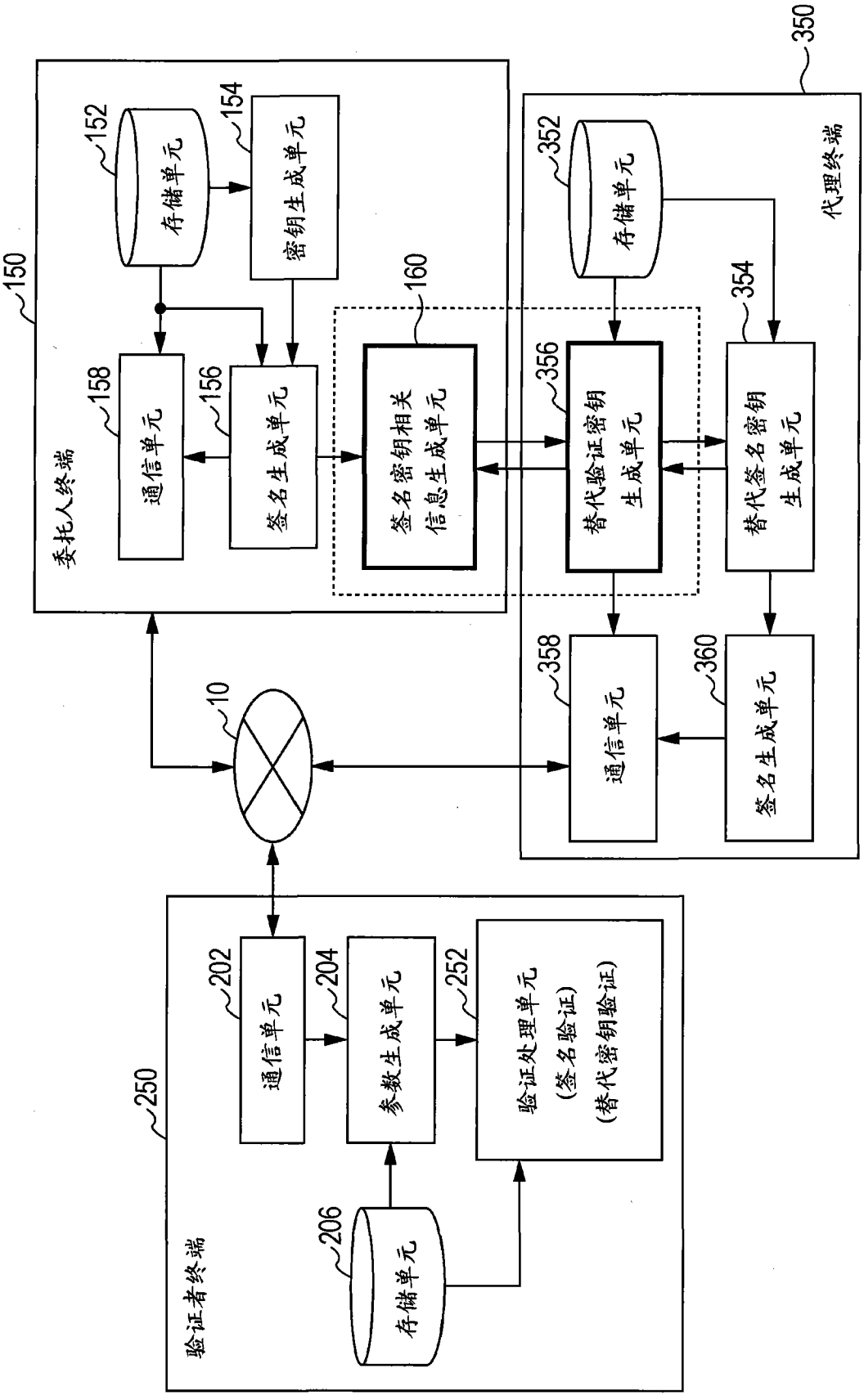

150
委托人终端
152
存储单元
154
密钥生成单元
158
通信单元
156
签名生成单元
160
签名密钥相关信息生成单元
350
代理终端
352
存储单元
354
356
替代验证密钥生成单元
替代签名密钥生成单元
358
通信单元
360
签名生成单元
10
250
验证者终端
202
通信单元
204
参数生成单元
252
验证处理单元
(签名验证)
(替代密钥验证)
206
存储单元

图 23

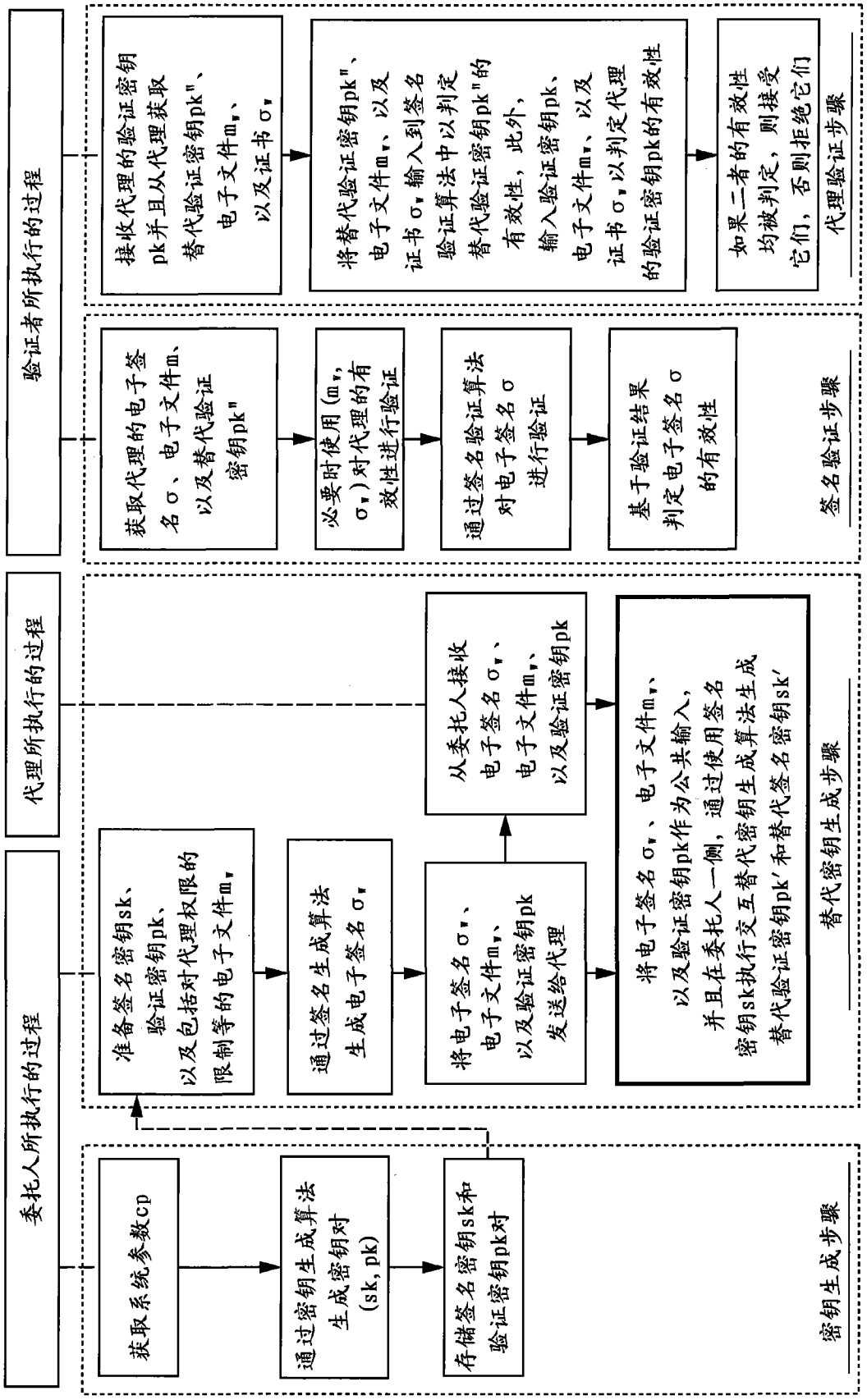

委托人所执行的过程
代理所执行的过程
验证者所执行的过程
获取系统参数cp
通过密钥生成算法
生成密钥对
(sk, pk)
存储签名密钥sk和
验证密钥pk对
密钥生成步骤
准备签名密钥sk、
验证密钥pk、
以及包括对代理权限的
限制等的电子文件m_w
通过签名生成算法
生成电子签名σ_w
将电子签名σ_w、
电子文件m_w、
以及验证密钥pk
发送给代理
从委托人接收
电子签名σ_w、
电子文件m_w、
以及验证密钥pk
将电子签名σ_w、电子文件m_w、
以及验证密钥pk作为公共输入，
并且在委托人一侧，通过使用签名
密钥sk执行交互替代密钥生成算法生成
替代验证密钥pk′和替代签名密钥sk′
替代密钥生成步骤
获取代理的电子签
名σ、电子文件m、
以及替代验证
密钥pk"
必要时使用(m_w,
σ_w)对代理的有
效性进行验证
通过签名验证算法
对电子签名σ
进行验证
基于验证结果
判定电子签名σ
的有效性
签名验证步骤
接收代理的验证密钥
pk并且从代理获取
替代验证密钥pk"、
电子文件m_w、
以及证书σ_w
将替代验证密钥pk"、
电子文件m_w、以及
证书σ_w输入到签名
验证算法中以判定
替代验证密钥pk"的
有效性，此外，
输入验证密钥pk、
电子文件m_w、以及
证书σ_w以判定代理
的验证密钥pk的有效性
如果二者的有效性
均被判定，则接受
它们，否则拒绝它们
代理验证步骤

图 24