



(12) 发明专利申请

(10) 申请公布号 CN 118104188 A

(43) 申请公布日 2024. 05. 28

(21) 申请号 202280069628.X

(22) 申请日 2022.10.26

(30) 优先权数据

10202112269T 2021.11.05 SG

(85) PCT国际申请进入国家阶段日

2024.04.16

(86) PCT国际申请的申请数据

PCT/SG2022/050769 2022.10.26

(87) PCT国际申请的公布数据

W02023/080842 EN 2023.05.11

(71) 申请人 pQCee私人有限公司

地址 新加坡新加坡

(72) 发明人 T·G·陈 J·周

(74) 专利代理机构 北京世峰知识产权代理有限公司 11713

专利代理师 卓霖 许向彤

(51) Int.Cl.

H04L 9/32 (2006.01)

G06F 21/64 (2006.01)

权利要求书2页 说明书9页 附图5页

(54) 发明名称

用于保护数字签名的方法和系统

(57) 摘要

提供了一种用于抗量子数字签名数据的方法、一种通过验证私钥来验证抗量子数字签名以认证数据源的方法、以及一种抗量子数字签名系统。所述抗量子数字签名系统包括数字签名系统和抗量子保护层。所述数字签名系统包括公钥和私钥，其中所述公钥与私钥相关联。所述数字签名系统还包括响应于数据和私钥生成的数字签名。所述抗量子保护层应用于数字签名系统，并且包括由签名方提供的关于私钥的预映射的量子安全知识证明。

算法2: 抗量子ECDSA签名 $Sign_q$.

```
1 开始
2  $G \leftarrow$  ECC 基点;  $P \leftarrow$  ECC 次序;
3  $\rho \leftarrow$  秘密预映射;
4  $M \leftarrow$  消息;
5 生成随机签名  $r$ ;
6 计算  $r^{-1}$  其中  $r \cdot r^{-1} \equiv 1 \pmod{P}$ ;
7 计算  $R = (R_x, R_y)$  其中  $R \equiv r \cdot G \pmod{P}$ ;
8 计算消息的散列值  $H(M)$ ;
9 列举ZKBoo证明  $\pi$  开始
10 零知识计算私钥  $K_s$  其中  $K_s = H(\rho)$ ;
11 零知识计算公钥  $K_p$  其中  $K_p \equiv K_s \cdot G \pmod{P}$ ;
12 计算  $s$  其中  $s \equiv r^{-1} \cdot (H(M) + R_x \cdot K_s) \pmod{P}$ ;
13 在证明中提交  $R_x, s$ ;
14 结束
15 销毁  $r, r^{-1}, K_s$ ;
16 返回  $\sigma = \{R_x, s\}, \pi$ ;
17 结束
```

1. 一种抗量子数字签名系统,包括:
数字签名系统,该数字签名系统包括公钥和私钥,其中所述公钥与所述私钥相关联,并且其中所述数字签名系统包括响应于数据和所述私钥生成的数字签名;以及
应用于所述数字签名系统的抗量子抗保护层,所述抗量子保护层包括签名方提供的关于所述私钥的预映射的量子安全知识证明。
2. 根据权利要求1所述的抗量子数字签名系统,其中,所述私钥的计算包括折叠散列函数。
3. 根据权利要求1和权利要求2所述的抗量子数字签名系统,其中,具有预定强度的加密密钥生成所述公钥和所述私钥两者。
4. 根据权利要求1至3中任一项所述的抗量子数字签名系统,其中,由签名方提供的关于所述私钥的预映射的量子安全知识证明包括零知识证明。
5. 根据权利要求1至3中任一项所述的抗量子数字签名系统,其中,由签名方提供的关于所述私钥的预映射的量子安全知识证明包括部分知识证明。
6. 根据权利要求1至5中任一项所述的抗量子数字签名系统,其中,由签名方提供的关于所述私钥的预映射的量子安全知识证明是响应于所述私钥的至少一部分而生成的。
7. 根据权利要求1至6中任一项所述的抗量子数字签名系统,其中,所述抗量子保护层通过提供所述私钥的预映射的多个知识证明来支持多于一方,所述私钥的预映射的多个知识证明具有预定义的证书层次结构。
8. 一种用于抗量子数字签名数据的方法,包括:
响应于安全参数来生成公钥和预映射参数;
生成私钥,其中所述私钥响应于所述预映射参数而生成并且与所述公钥相关联;
响应于数据和所述私钥来生成签名;
生成所述预映射参数的知识证明;以及
利用所述签名和所述预映射参数的知识证明两者对所述数据进行数字签名。
9. 根据权利要求8所述的方法,其中,对所述数据进行数字签名包括将所述签名与零知识证明分开存储,以便并行验证。
10. 根据权利要求8或权利要求9所述的方法,其中,生成所述私钥包括使用折叠散列函数来生成所述私钥。
11. 根据权利要求8至10中任一项所述的方法,其中,所述安全参数包括具有预定强度的加密密钥。
12. 根据权利要求8至11中任一项所述的方法,其中,所述预映射参数的知识证明包括零知识证明。
13. 根据权利要求8至11中任一项所述的方法,其中,所述预映射参数的知识证明包括部分知识证明。
14. 根据权利要求8至13中任一项所述的方法,其中,所述预映射参数的知识证明是响应于所述私钥的至少一部分而生成的。
15. 根据权利要求8至14中任一项所述的方法,其中,生成所述私钥包括通过对所述预映射参数执行散列密钥推导、对所述预映射参数执行单向函数密钥推导、或者对所述预映射参数执行对称密钥推导来生成所述私钥中的一种或多种。

16. 根据权利要求8至15中任一项所述的方法, 其中, 生成所述公钥和所述预映射参数包括通过对所述预映射参数执行散列密钥推导来生成所述公钥、通过对所述预映射参数执行单向函数密钥推导来生成所述公钥、或者通过对所述预映射参数执行对称密钥推导来生成所述公钥中的一种或多种。

17. 根据权利要求8至16中任一项所述的方法, 其中, 所述数据包括消息, 所述方法还包括发送数字签名消息, 其中所述预映射参数的知识证明是由所述消息的接收者可访问的。

18. 根据权利要求17所述的方法, 其中, 发送所述数字签名消息包括与 (i) 所述预映射参数的知识证明或 (ii) 用于识别数字存储位置的位置信息中的一个或两个一起发送数字签名消息, 从所述数字存储位置能够访问所述预映射参数的知识证明。

19. 根据权利要求17或权利要求18所述的方法, 还包括发送所述公钥, 其中发送所述公钥包括将数字签名消息与所述公钥一起发送到数字存储位置或将所述公钥发送到数字存储位置, 所述数字存储位置包括认证机构或公共存储库。

20. 一种通过验证私钥来验证抗量子数字签名以认证数据源的方法, 所述方法包括:
通过使用与所述私钥相关联的公钥和预映射参数的知识证明两者进行验证以验证与所述数据对应的数字签名是否是响应于所述私钥而生成的, 来认证所述数据源。

21. 根据权利要求20所述的方法, 其中, 所述预映射参数的知识证明包括零知识证明。

22. 根据权利要求20和权利要求21所述的方法, 其中, 认证步骤包括并行处理使用所述公钥进行的验证和使用所述预映射参数的知识证明进行的验证。

23. 根据权利要求22所述的方法, 其中, 并行处理使用所述公钥进行的验证和使用所述预映射参数的知识证明进行的验证包括:

从第一数字存储位置提取所述公钥; 以及

从第二数字存储位置提取所述预映射参数的知识证明。

24. 根据权利要求20至23中任一项所述的方法, 其中, 对数据源进行认证包括当且仅当所述数字签名被确定为是响应于所述私钥而生成的、并且所述预映射参数的知识证明被确定为是根据所述预映射参数计算的有效证明两者时, 接受对所述数据的验证。

用于保护数字签名的方法和系统

[0001] 优先权要求

[0002] 本申请要求于2021年11月05日提交的申请号为10202112269T的新加坡专利申请的优先权。

技术领域

[0003] 本发明总体上涉及数字签名,并且更具体地涉及用于保护数字签名以抵抗具有量子能力的对手的方法和系统。

背景技术

[0004] 非对称密钥加密法是由全世界的系统使用以维护数字领域中各方之间信任的工具。数字签名的使用使通信各方能够彼此认证、检查所交换数据的完整性、并且在否认的情况下证明数据的来源。美国国家标准与技术研究院(NIST)的数字签名标准中描述了三种经典的数字签名算法,并且这三种经典的数字签名算法包括基于离散对数加密法的数字签名算法(DSA)、里维斯特-沙米尔-阿德尔曼(RSA)算法、和基于椭圆曲线加密法(ECC)椭圆曲线数字签名算法(ECDSA)。DSA和ECDSA的安全性基于在超大数的有限域上求解离散对数,而RSA的安全性则基于在超大数的有限域上进行整数分解的难度。

[0005] 然而,大型容错量子计算机的出现给使用这些经典数字签名算法的系统带来了巨大风险。秀尔算法在 $O(\log N)$ 多项式时间内既能解决DSA和ECDSA所基于的离散对数问题,也能解决RSA所基于的整数分解问题。这意味着,任何拥有足够大的量子计算机的对手,在得到用户公钥的情况下,都能在数小时内计算出用户的私人签名密钥,并且由此生成有效的数字签名来冒充所述用户。此外,之前由所述用户签名的数据也无法再证明其真实性和可信性。

[0006] 虽然随着新数字签名标准的发展,业界可能会鼓励新的系统实施方案来考虑,但是现有或即将推出的系统所面临的挑战提出了以下专门针对数字签名的问题:面对量子计算机数字签名击溃能力,已经数字签名的文件如何保持可信性?这些文件是否需要使用新算法进行会签?由于会签人可能是交易中无利害关系的第三方,那么会签人要为验证方承担什么责任?无法迁移的遗留系统怎么办?验证方预计何时准备好验证新算法?如果现有的非量子安全签名通过了验证,但验证方无法验证新的量子安全签名,这对验证方有何法律影响?使用数字签名的系统运营商是否应该开始向基于散列的有状态的签名进行加密迁移,而不是等待行业标准化?

[0007] 因此,需要用于数字签名的系统和方法,以克服现有数字签名系统的缺点并保护数字签名免受具有量子能力的对手的影响。此外,其他期望的特征和特性将从随后的详细描述和所附权利要求书并结合本公开的附图和上述背景技术而变得显而易见。

发明内容

[0008] 根据本发明实施例的至少一个方面,提供了一种抗量子数字签名系统。该抗量子

数字签名系统包括数字签名系统和抗量子保护层。所述数字签名系统包括公钥和私钥,其中所述公钥与所述私钥相关联。所述数字签名系统还包括响应于数据和所述私钥生成的数字签名。所述抗量子保护层适用于数字签名系统,并且包括由签名方提供的关于所述私钥的预映射的量子安全知识证明。

[0009] 根据本发明实施例的另一方面,提供了一种用于抗量子数字签名数据的方法。该方法响应于安全参数生成公钥和预映射参数,并且生成私钥,其中所述私钥是响应于所述预映射参数生成的并且与所述公钥相关联。该方法还包括:响应于数据和所述私钥而生成签名;生成预映射参数的知识证明;以及利用签名和预映射参数的知识证明两者对所述数据进行数字签名。

[0010] 根据本发明实施例的另一个方面,提供了一种通过验证私钥来验证抗量子数字签名以认证数据源的方法。该方法包括通过使用与私钥相关联的公钥和预映射参数的知识证明两者进行验证以验证与数据对应的数字签名是否响应于私钥而生成,来认证所述数据源。

附图说明

[0011] 在附图中,相同的附图标记指代在各个分开的视图中相同或功能相似的元件,这些附图与下文的详细描述一起并入本说明书中并且构成本说明书的一部分,用于示出各种实施例并解释根据本发明实施例的各种原理和优点。

[0012] 图1描绘了根据本发明实施例的示例性抗量子ECDSA密钥生成算法 KeyGen_q 。

[0013] 图2描绘了根据本发明实施例的示例性抗量子ECDSA签名算法 Sign_q 。

[0014] 图3描绘了根据本发明实施例的示例性抗量子ECDSA验证算法 Verify_q 。

[0015] 图4描绘了示出根据处于测试中的本发明实施例的抗量子数字签名方案的实际实施方案的用例的过程图。

[0016] 图5描绘了在根据本发明实施例的抗量子数字签名方案的实际实施方案中例示出预定义证书层次结构的窗口的图像。

[0017] 而图6描绘了在根据本发明实施例的抗量子数字签名方案的实际实施方案中例示出由时间戳客户端验证的窗口的图像。

[0018] 本领域技术人员可以理解,附图中的元件是为了简单明了而示出的,并且不一定按比例绘制。

具体实施方式

[0019] 下面的详细描述只是示例性的,并且不旨在限制本发明或本发明的应用和用途。此外,本发明不旨在受前面的背景技术部分或下面的详细描述中提出的任何理论的约束。本发明实施例旨在提出一种新的手段,为使用RSA/DSA/ECDSA和其他数字签名算法的系统增加抗量子保护层,否则这些系统可能会受到使用量子计算机的对手的攻击。根据本发明的实施例,使用量子安全零知识证明将要求签名方包含关于私钥确实由签名方生成而非使用量子计算机加密分析的证明。这根据本发明实施例的方法和系统由签名方实现,在签名过程中,在对要发送给验证方的消息进行数字签名时,签名方包括对私钥的预映射的知识的量子安全零知识证明以及由所述私钥生成的数字签名。通过这种方式,本发明实施例使

得使用RSA/DSA/ECDSA和其他数字签名算法的系统能够有利地实现保护以对抗量子计算机,同时与现有的验证方实施方案和认可使用数字签名的立法机构保持向后兼容性。

[0020] 根据本发明实施例的方法和系统基于以下前提而形成:如果现有的数字签名即使在足够大的量子计算机建成后仍能保持量子抗性,则可以避免许多与过渡相关的向后兼容性问题。向新算法迁移的时间表将不太依赖对手方,并且现有的数字签名文件在后量子时代有利地保持其真实性。本发明的实施例通过将私人签名密钥的预映射的量子安全零知识证明与签名一起分层,来有利地防止现有系统面临的兼容性问题,其技术效果是:(a)扩展数字签名方案,以构建具有向后兼容性特性的抗量子数字签名方案;(b)使用零知识证明来实现抗量子数字签名方案,该零知识证明待与数字签名一起提供,以使数字签名具有量子抗性;(c)部署真实世界的实施方案,该实施方案包括 Adobe® PDF 数字签名解决方案,该解决方案提供了与RFC3161兼容的时间戳服务器,以利用X.509.v3证书签发抗量子ECDSA时间戳数字签名,其中X.509.v3证书与现有的Adobe PDF Acrobat Reader DCv2021.x兼容。

[0021] 数字签名在数字通信中提供了完整性、真实性和不可否认性。例如,爱丽丝和鲍勃是通信双方。爱丽丝具有一条消息M要发送给鲍勃,并且希望确保鲍勃收到的消息没有任何变化(完整性),而且知道该消息来自爱丽丝(真实性)。鲍勃希望能够向第三方证明该消息确实来自爱丽丝(不可否认性)。

[0022] 数字签名方案被定义为多项式时间算法KeyGen、Sign和Verify的三重组合。KeyGen算法接收安全参数 1^n ,该安全参数定义了预定强度为n的加密密钥强度,并且输出私钥 K_s 和相应的公钥 K_p 。Sign算法接收消息M和私钥 K_s ,并且输出签名 σ 。并且Verify算法接收消息M、公钥 K_p 和签名 σ ,当且仅当 σ 是由Sign(M, K_s)生成的有效签名时,才输出“接受”。这些关系如等式(1)、(2)和(3)中所示。

$$[0023] \quad \text{KeyGen}(1^n) \Rightarrow \{K_s, K_p\} \quad (1)$$

$$[0024] \quad \text{Sign}(M, K_s) \Rightarrow \{\sigma\} \quad (2)$$

$$[0025] \quad \text{Verify}(M, K_p, \sigma) \Rightarrow \{\text{结果}\} \quad (3)$$

[0026] 在爱丽丝和鲍勃的示例中,爱丽丝(签名方)调用KeyGen生成 $\{K_s, K_p\}$ 。 K_p 发布后,鲍勃和其他各方都能访问 K_p 。然后,爱丽丝利用自己的私钥 K_s 调用Sign来签署消息M,从而生成签名 σ 。爱丽丝将 $\{M, \sigma\}$ 传送给鲍勃。鲍勃(验证方)使用爱丽丝的公钥 K_p 调用Verify来验证消息M的签名 σ 。如果Verify返回“接受”,则鲍勃成功地从爱丽丝处接收到了未改变的消息M和签名证明 σ 。

[0027] 零知识证明被定义为:除了命题的正确性外,不传递任何额外的知识证明。尽管零知识证明具有很多具体的实现方式,但是抗量子的非交互式零知识证明要么是基于ZKStark的证明,要么是基于MPC-in-the-head(多方头部计算)的证明。部分知识证明是指:除了命题的正确性之外,还传递一些知识的证明。

[0028] 对于MPC-in-the-head证明,证明者必须创建具有承诺的n个分支的布尔计算电路,其中n-1个视图可以作为知识证明透露给验证者。为了使证明为非交互式,证明者可以使用菲亚特-沙米尔启发式,以利用确定但不可预测的方式来决定将哪些n-1个视图发送给验证者。然后,验证者浏览所述n-1个视图,有 $\frac{1}{n}$ 的机会确定命题是否错误。通过增加验证者

必须计算所述电路并且提供视图的回合数(采用不同的随机输入参数),验证者提出错误请求的统计概率就会呈指数级下降。

[0029] 由于量子计算机上的秀尔算法破解了整数分解问题、离散对数问题和椭圆曲线离散对数问题,因此可以有把握地假定,当制造出足够大的量子计算机时,对手可以在给定公钥 K_p 的情况下计算出所有RSA/DSA/ECDSA私钥 K_s 。然而,对称密钥和基于散列的加密法仍然相对具有量子抗性。例如,量子计算机上的格罗弗算法在执行蛮力搜索时只能达到 $O(\sqrt{N})$ 的二次加速,并且这已被证明是最优的。

[0030] 因此,根据本发明的实施例,签名过程被扩展到在对私钥的预映射的知识的零知识证明中的层,以保护签名。然后,扩展的验证过程可以验证该证明,以确定所述签名是由私钥所有者(而非具有量子能力的对手)真正创建的。为了向后兼容,现有的验证过程仍然可以在没有所述证明的情况下验证数字签名,尽管失去了抗量子保证。

[0031] 为了实施根据本发明实施例的有利解决方案,对经典数字签名方案的三重多项式时间算法(即公式(1)、(2)和(3))进行了扩展。根据本发明实施例的扩展的抗量子数字签名方案被定义为三重多项式时间算法 $KeyGen_q$ 、 $Sign_q$ 和 $Verify_q$ 。算法 $KeyGen_q$ 接收用于定义 n 的加密密钥强度的安全参数 1^n ,并且输出秘密预映射参数、预映射 ρ 和公钥 K_p 。 K_p 是与私钥 $H(\rho)$ 相关联的公钥,其中私钥的计算 $H()$ 是一个折叠散列函数。算法 $Sign_q$ 接收消息 M 和秘密预映射 ρ ,并且输出使用 $Sign(M, H(\rho))$ 计算的签名 σ 以及抗量子零知识证明 π ,其中 $H(\rho)$ 由 ρ 计算, σ 由 $H(\rho)$ 计算,并且抗量子零知识证明 π 是响应于至少一部分私钥 $H(\rho)$ 而生成的。私钥 $H(\rho)$ 可以通过对预映射 ρ 执行散列密钥推导、对预映射 ρ 执行单向函数密钥推导、或者对预映射 ρ 执行对称密钥推导来生成。由于公钥 K_p 与私钥 $H(\rho)$ 相关联,因此公钥 K_p 也可以通过对预映射 ρ 执行散列密钥推导、对预映射 ρ 执行单向函数密钥推导、或者对预映射 ρ 执行对称密钥推导来生成。

[0032] 为了验证,算法 $Verify_q$ 接收消息 M 、公钥 K_p 和签名 σ ,并且当且仅当 $Verify(M, K_p)$ 返回接受且 π 是知识的有效零知识证明时,输出“接受”以认证所述消息 M 的来源,其中 σ 是根据 ρ 计算的。这些关系在等式(4)、(5)和(6)中示出。

$$[0033] \quad KeyGen_q(1^n) \Rightarrow \{\rho, K_p\} \quad (4)$$

$$[0034] \quad Sign_q(M, \rho) \Rightarrow \{\sigma, \pi\} \quad (5)$$

$$[0035] \quad Verify_q(M, K_p, \sigma, \pi) \Rightarrow \{\text{结果}\} \quad (6)$$

[0036] 直观地说,根据本发明实施例的数字签名方案继承了经典数字签名方案的经典安全特性,并在私钥上附加了抗量子层。由于从 $Sign_q$ 获取的附加信息是不会泄露秘密预映射 ρ 或私钥 $K_s = H(\rho)$ 的零知识证明,因此经典对手在与签名方交互时无法破坏 $Verify_q$ 的可靠性。

[0037] 因此,可以看出,根据本发明实施例的抗量子数字签名方案可以为使用 $Sign_q$ 生成的数字签名提供额外的量子抗性,前提是使用 $Verify_q$ 验证所述签名 σ 和证明 π ,其中证明 π 是签名方提供的关于私钥的预映射 ρ 的量子安全知识证明,因此,使用可由验证者访问的证明 π 来量子安全地证明:所述数字签名 σ 是根据 ρ 计算的。

[0038] 通过假定具有量子能力的对手能够使用秀尔算法从 K_p 中恢复 $H(\rho)$,可以证明根据

本发明实施例的数字签名方案具有额外的量子抗性。利用 $H(\rho)$, 对手能够使用 Sign 任意生成有效的签名 σ , 这些签名将被 Verify 接受。然而, 对手将无法生成所述证明 π , 因为通过计算私钥 $H(\rho)$ 无法恢复签名 ρ 的值, 因为 $H()$ 是折叠散列函数并且可以抵抗预映射攻击, 即使是来自量子计算机的攻击。因此, Verify_q 可以抵抗具有量子能力的对手。

[0039] 此外, 可以看出, 使用根据本发明实施例的数字签名方案的 KeyGen_q 和 Sign_q 的签名方有利地生成签名 σ , 所述签名 σ 是与使用经典数字签名方案的 Verify 算法的验证方向后兼容的。

[0040] 根据本发明实施例的抗量子数字签名方案的向后兼容性由以下事实体现: Sign_q 返回的签名 σ 是使用相同算法 Sign 生成的, 其中 $H(\rho)$ 实际上等于 K_s 。因此, 使用 Verify 的任何验证方将可以忽略 π , 并且继续调用 Verify 来检查签名 σ 相对于 M 和 K_p 的有效性。

[0041] 因此, 可以看出, 根据本发明的实施例, 包括了数字签名算法、散列函数和零知识证明系统, 以实现抗量子数字签名方案。

[0042] 可以方便地使用DSA或ECDSA作为根据本发明实施例的抗量子数字签名方案的数字签名算法。这是因为DSA和ECDSA的私钥生成器本质上是在有限域上生成的不可预测的随机数, 该随机数有利地与单向散列函数 $H()$ 的输出非常匹配。使用RSA作为签名算法则更为复杂和繁琐, 因为密钥生成涉及将散列函数的输出与两个以上的用于计算RSA模数的不可预测质数相匹配。可能的技术包括将散列输出映射到由非常大的质数组成的有序列表中或者重复散列(或挖掘)随机数直到找到质数。对于更简单的实施方案, 可以使用ECDSA, 因为其具有最小的密钥尺寸, 这转化为最小的证明尺寸, 并且待选择的可行曲线可以是用于本文的实施方案示例的secp256r1(或prime256v1)。

[0043] 根据本发明实施例待使用的并且用于本文的实施方案示例的散列函数是SHA-256, 因为它是折叠函数, 并且其输出与secp256r1曲线非常匹配。

[0044] 根据本发明实施例的抗量子数字签名方案中待使用的零知识证明系统必须是后量子安全的。ZKBoo就是这样一种零知识证明系统, 因为它是三分支MPC-in-the-head实现, 并且已经具有现成的SHA-256实施方案。因此, ZKBoo被用作本文的实施方案示例的零知识证明系统。

[0045] 参照图1, 示出了根据本发明实施例的示例性抗量子ECDSA密钥生成算法 KeyGen_q 100。密钥生成算法 KeyGen_q 100的功能与 KeyGen 非常相似, 除了额外的步骤110(参见步骤4)之外, 该步骤110是在计算公钥 K_p 之前对秘密预映射 ρ 进行散列。

[0046] 参照图2, 示出了根据本发明实施例的示例性抗量子ECDSA签名算法 Sign_q 200。除了使用私钥 $H(\rho)$ 计算ECDSA签名之外, Sign_q 函数还返回ZKBoo证明 π , 该ZKBoo证明 π 包括对 $H(\rho)$ 的预映射的知识的零知识证明、根据 $H(\rho)$ 计算公钥 K_p 的零知识证明、以及 $H(M)$ 是被签名的消息的承诺。

[0047] 根据本发明实施例的该实施方案在步骤210(步骤10)处使用贾科梅利SHA-256代码。在下一步骤220(步骤11)的代码需要特别注意, 因为在证明 π 中的计算步骤数可能会泄露私钥 K_s 。例如, 当在已生成私钥 K_s 后计算公钥 K_p 时, 用于椭圆曲线加密法(ECC)的等式为 $K_p = K_s \cdot G \bmod P$, 其中 G 是在椭圆曲线上的已知基点, P 是所述曲线的阶数。在正常计算情况下, G 将由 K_s 相乘的点积。由于 K_s 的值介于1到 2^{256} 之间, 并且乘法采用比特移位法(bit shift method), 因此需要进行1到256次点积乘法才能得到 K_p 。根据MPC-in-the-head零知

识证明, 计算 K_p 所需的电路的门数将显示在所述证明中, 这意味着如果有人分析证明电路的尺寸, K_s 的值就会被揭示出来。因此, 根据本发明的实施例并且为了进一步有利地屏蔽/隐藏私钥 K_s 的值, 而创建了一种电路, 无论 K_s 的值如何, 该电路都会执行预定次数的点积乘法, 从而使在公钥计算中的电路数量保持不变。在本实施方案中, 由于椭圆曲线是secp256r1曲线, 因此预定的计算次数为256次。此外, 在执行椭圆曲线乘法时, 有利地实施蒙哥马利阶梯始终加倍并相加(Montgomery ladder double-and-add always technique)技术, 以增加进一步的安全级别并且防止定时和功率侧信道攻击, 即攻击者测量在从私钥计算公钥时的时间或功率消耗。

[0048] 参照图3, 示出了根据本发明实施例的示例性抗量子ECDSA验证算法Verify_q 300。

[0049] 抗量子ECDSA验证算法Verify_q 300包括两部分, 其中第一部分310 (从步骤5到步骤12) 是类似于Verify的ECDSA签名验证, 而第二部分320 (从步骤14到步骤20) 是根据本发明实施例的抗量子零知识证明的附加验证。

[0050] 根据本发明实施例的抗量子数字签名方案的示例性实施方案是用C语言实现的, 并且在英特尔I5-8250U第八代机器上进行了测试, 该机器具有8个CPU内核和8GB内存, 并且在64位微软Windows 10上运行Cygwin终端。没有进行操作系统级的CPU排程或调整。测量了以及在ZKBoo轮数从50到250以50为增量变化时Sign_q和Verify_q的执行时间、所述证明的尺寸。如表1所示, 增加轮数会增加证明的位强度, 但是也会无意中增加所述证明的尺寸和执行时间。

[0051]	ZKBoo 轮数	50	100	150	200	250
	证明大小 (以千字节计)	1,978	3,956	5,934	7,912	9,890
	Sign _q 执行时间 (以秒计)	20.9	45.9	72.9	95.1	118.2
	Verify _q 执行时间 (以秒计)	19.6	45.0	71.0	93.2	115.7

[0052] 表1

[0053] 乍一看, 用于250位强度证明的测量开销显示出证明非常大, 大小约为10MB, 并且需要差不多两分钟来执行Sign_q或者Verify_q。然而, 根据下文讨论的本发明实施例的抗量子数字签名方案的实际部署实施方案能够减少对用户体验的影响, 因为所述证明可以异步生成, 并且与所述证书分开存储 (即其中所述证明存储在第一数字位置, 而所述证书存储在第二数字位置)。这可以有利地使能并行处理或异步验证, 以附加地减少对用户体验的影响。

[0054] 为了研究与向后兼容性和向抗量子迁移相关的问题, 根据本发明实施例的抗量子数字签名方案被部署到时间戳服务器中, 同时使用现有的 (未改变的) Adobe Acrobat Reader DC来请求抗量子时间戳签名的PDF, 作为抗量子数字签名方案的实际部署实施方案。上述部署是在笔记本电脑上进行的, 该笔记本电脑配备英特尔I5-8250U第八代机器, 该机器具有8个CPU内核和8GB内存, 对于客户端和服务端两者均运行64位Microsoft Windows 10操作系统。设置包括时间戳客户端和时间戳服务器。对于时间戳客户端, 使用Adobe Acrobat Reader DC v2021.x (因为该客户端已经支持ECDSA), 并且能够在未修改的情况下使用。对于时间戳服务器, 使用Pierre-Francois Carpentier的开源时间戳服务器 (来自<https://github.com/kakwa/uts-server>), 其中代码未经修改。

[0055] 对于加密库,时间戳服务器使用OpenSSL v1.1.x来执行认证机构(CA)签发服务器证书的操作,以及根据RFC3161执行数字签名。对OpenSSL v1.1.1b的版本进行了修改,以执行对于X.509证书签发和加时间戳两者的扩展数字签名方案。对OpenSSL进行了优化,以使其在异步生成ZKBoo证明的同时返回ECDSA签名。这允许将ECDSA签名时间戳返回到客户端,而无需等待ZKBoo证明完全生成。因此,所述证明与证书被分开地存储。

[0056] 由于用于所述证书和时间戳的抗量子256轮ZKBoo证明的每一个都是10MB字节,因此可能无法容易地将它们传输到客户端。因此,修改版OpenSSL将所述证明写入Dropbox (www.dropbox.com),同时将URL链接嵌入签名的X.509证书或返回到调用程序的PKCS#7时间戳中。

[0057] 参照图4,流程图400示出了根据本发明实施例进行测试的抗量子数字签名方案的实际实施方案的用例。如上所述,该实施方案使终端用户401能够使用Adobe Acrobat Reader 402作为时间戳客户端。该实施方案还包括时间戳服务器404,该服务器使用OpenSSL 406进行证书签发和加时间戳,OpenSSL 406将所述证明写入Dropbox 408。

[0058] 在仅进行一次的设置阶段410,OpenSSL 406用于生成412用于根CA证书的密钥和证书,并且用于生成414用于时间戳服务器证书的密钥和证书。如图5的图像500中的窗口510、520所示,采用根据本发明实施例定义的证书层次结构,其中根CA将对服务器证书进行认证,而无需中间CA。两个证书都包括在X.509Authority-Information-Access(授权信息访问)扩展下的链接416、418,作为数字存储位置信息,以指向在Dropbox408中的抗量子证明。在操作中,所述数字存储位置可以是由使用所述数字存储位置信息的验证者能够访问的认证机构或公共存储库。将根CA证书下载420至终端用户401,然后导入422至Adobe Acrobat 402,以建立信任根。

[0059] 在RFC3161阶段430中,在终端用户401打开432PDF文件后,可以通过从Adobe Acrobat 402向时间戳服务器404发起434请求来为PDF文件加时间戳。时间戳服务器404向OpenSSL 406发送请求436,并且接收438ECDSA签名PKCS#7时间戳,该时间戳被提供440给Adobe Acrobat402。时间戳签名证明442同样存储在Dropbox 408中,其中在时间戳中嵌入了URL链接。该时间戳可以由Adobe Acrobat 402验证444并且被保存在PDF中,以供终端用户401稍后认证446。在图6的图像600中示出了所述验证的示例。注意,未经修改的Adobe Acrobat仅验证ECDSA签名的时间戳和证书链,而不验证ZKBoo证明,因此终端用户经历的等待时间没有变化。

[0060] 在升级后阶段450,任何能够运行Verify_q的验证方可以跟从452在所述证书/签名块中发现的链接以下载454抗量子证明,以根据抗量子ECDSA验证算法300(图3)完成签名验证。

[0061] 为了了解逐步迁移到抗量子数字签名方案对系统的影响,表2中列出了在不同迁移阶段对于签名方和验证方的不同结果。从表2中可以看出,根据本发明实施例的抗量子层的适当迁移策略是首先升级签名方,以使签名中包含抗量子证明,然后再升级验证方,以使其能够验证所述证明。对于选择提前升级的验证方,建议其根据上文讨论的经典数字签名方案加入Verify功能,以保持与可能尚未升级的签名方的兼容性。

		验证方	
		定义 1 ¹	定义 2 ²
[0062]	签名方	定义 1 ¹ 这是“原样”情况。在后量子时代，签名文件很容易被伪造。	签名文件不包括抗量子证明。验证方可以选择拒绝接受文件或使用 <i>verify</i> 来检查签名，同时通知签名方进行迁移。
		定义 2 ² 这是迁移过程中适当的“步骤 1”。签名文件包括	这是“未来”状态，并且是迁移过程中适当的
[0063]		抗量子证明。签名方无需等待验证方在完成迁移之后再执行此步骤。验证方继续验证签名，同时忽略抗量子证明。	“步骤 2”。在签名方已完成迁移并开始发送包括抗量子证明的已签名文件之后，验证方可以更新他们的系统以验证签名和证明，以完成迁移过程。
[0064]	¹ 尚未迁移。仍在使用定义1的KeyGen、Sign和Verify。		
[0065]	² 迁移已完成。使用定义2的KeyGen、Sign和Verify进行升级。		
[0066]	表2		
[0067]	根据本发明实施例的抗量子数字签名方案的优点对于本领域技术人员来说是显而易见的,并且可以通过当今的技术实现。随着更强大的量子计算机上线,后量子最终期限即将到来,并且根据本发明实施例的抗量子数字签名方案的优势将成为安全、可认证通信的必要条件。作为后量子最终期限的参考,NIST提供了一份报告,其中提到到2030年,很可能用10亿美元的预算就能制造出一台能够加密RSA-2048的量子计算机。为了解决这个问题,NIST正在开展后量子标准化工作,以选择合适的量子安全数字签名和密钥交换算法。预计最终选择工作将很快完成,其中新标准将于2024年公布。另外,NIST还推荐了两种基于散列的有状态的签名,即Leighton-Micali签名和eXtended-Merkle签名方案,供在一定条件下后量子使用。		
[0068]	虽然业界可能会鼓励2024年后的新系统实施方案考虑采用新的数字签名标准,但是预计现有或即将推出的系统将面临不同的挑战。		
[0069]	使数字签名实现量子安全的本能方案是使用替代或额外的量子安全算法。NIST的后量子标准化工作目前已确定两种基于格的算法(即:Dilithium和Falcon)以及一种基于多变量的算法(即:Rainbow)作为三种最终入围的数字签名算法。三种另选算法,即基于多变量的GeMSS、基于零知识的Picnic(该算法也使用在本发明实施例的实施方案中讨论的零		

知识证明系统ZKBoo作为创建ZKB++的底层证明系统)和基于散列的无状态SPHINCS+已入围,但是将在2024年最终期限之后接受进一步评估。理想的情况是,可以使用呈软件库或硬件安全模块的形式的“直接替代品”,以利用标准化的新算法来替换或增强RSA/DSA/ECDSA。但是,由于这些算法中的每一种都具有独特的资源、性能和平台考虑因素,再加上不同的密钥仪式过程和协议,因此更有可能需要设计和实施迁移手册。

[0070] 另一种方法是使用备份密钥,该备份密钥可以在发生泄露时覆盖常规签名密钥。一种建议是使用抗量子有状态的基于散列的W-OTS+备份密钥,该备份密钥在密钥生成过程中创建,并且可以在原始密钥泄露或丢失时用作后备程序。虽然这种备份数字签名密钥方案可以作为验证相关协议的账户恢复机制,但是它们并不适用于其中需要对数据进行长期不可否认保护的常规非交互式数字签名用例。

[0071] 具体到加时间戳用例,使用散列序列(即:在正向方向上或反向方向上对它们进行链式处理)是一种众所周知的提供长期的、可能是量子安全的加时间戳的方案,其可以包括通过线性散列链或通过梅克尔树来链接待加时间戳的文件序列而加数字时间戳。如今,诸如以太坊的区块链已经支持加时间戳智能合约,并且可以提供在区块链上的去中心化时间戳协议,该协议可以防止预先/事后记时间。由于这些技术通常依赖于公共可验证链来确定发生的具体时间,因此它们并不适用于作为保护一般数字签名的抗量子机制。公共区块链还面临与隐私相关的问题,因为所进行的交易数量和交易时间都是公开可得的。

[0072] 因此,可以看出,本发明的实施例提供了一种抗量子数字签名方案,该方案提供了一种当前的解决方案,该解决方案能够有利地并且有效地解决在安全和可认证通信中现有的和即将出现的问题。根据本发明实施例的抗量子数字签名方案在实施后量子数字签名时采用了不同的方法。根据本发明实施例的抗量子数字签名方案不是替换或附加不同的量子安全数字签名算法,而是使继续使用经典RSA、DSA或ECDSA数字签名算法成为可能,同时实现更长期的量子抗性。这是通过在数字签名之外对私钥的预映射的知识的零知识证明进行分层来实现的。通过根据本发明实施例的抗量子数字签名方案,希望在量子准备就绪方面取得进展的数字签名实施方案继续保持对现有应用的向后兼容性。这一点非常有利,因为不同的系统可能对何时迁移到量子就绪方面具有不同的时间线和时间表,而根据本发明实施例的抗量子数字签名方案能够确保在升级的和非升级的应用之间的无缝操作。

[0073] 尽管根据本发明实施例的抗量子数字签名方案的应用在上文针对示例性PDF文件加时间戳方案进行了讨论,但是其他应用,诸如区块链、安全电子邮件和传输层安全,也可以利用根据本发明实施例的数字签名方案在量子抗性中进行分层。

[0074] 尽管在本发明实施例的上述详细描述中介绍了示例性实施例,但是应当理解的是,还存在大量的变形。应进一步理解的是,示例性实施例仅为示例,并且不旨在以任何方式限制本发明的范围、适用性、操作或配置。相反,上述详细描述将为本领域技术人员提供用于实施本发明的示例性实施例的方便路线图,不言而喻,可以对示例性实施例中描述的步骤和操作功能的功能和布置进行各种更改,而不会偏离所附权利要求书中阐述的本发明的范围。

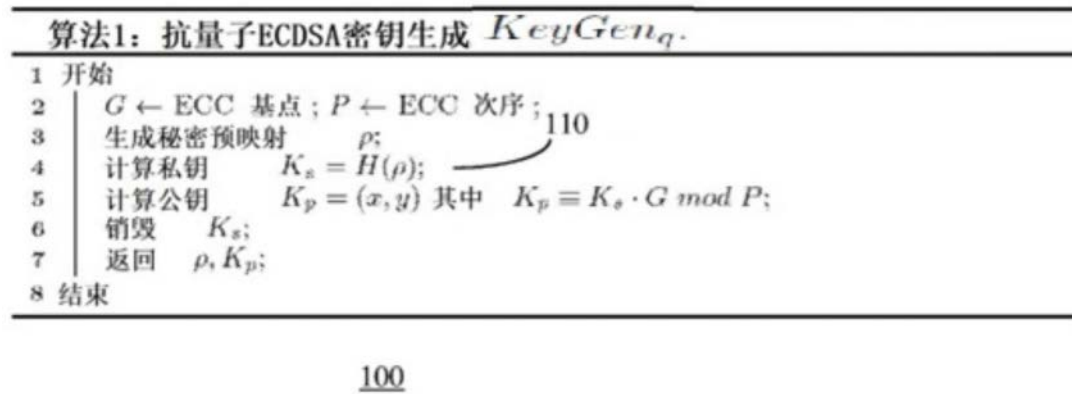


图1

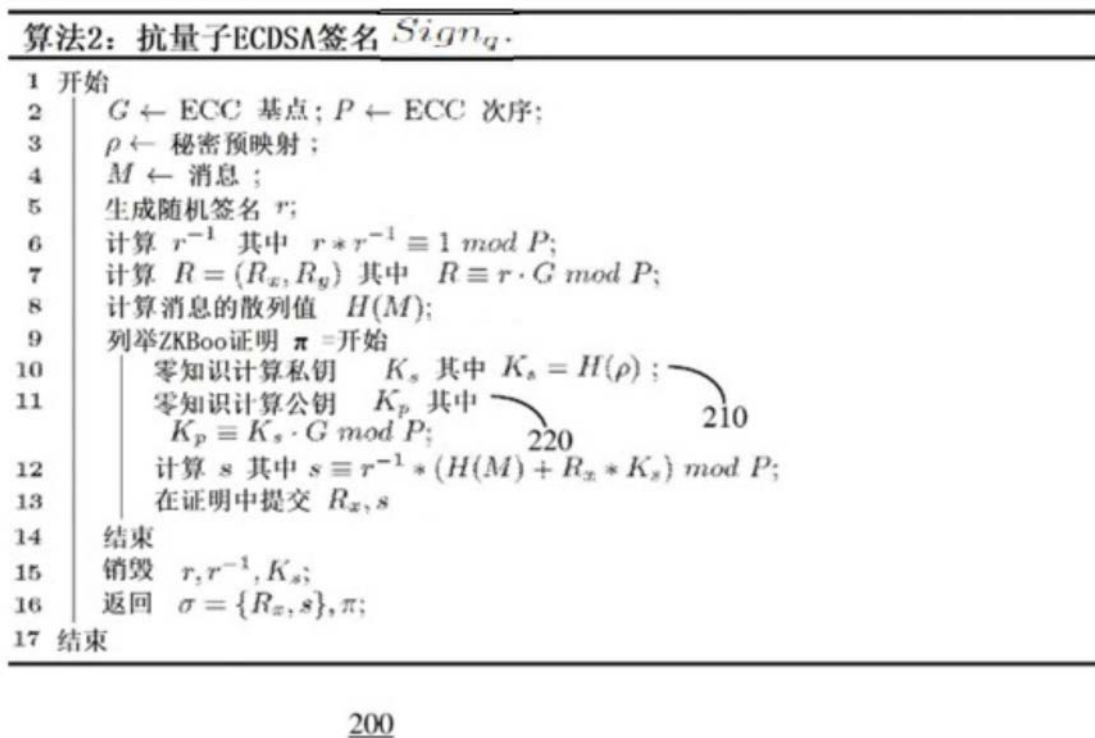


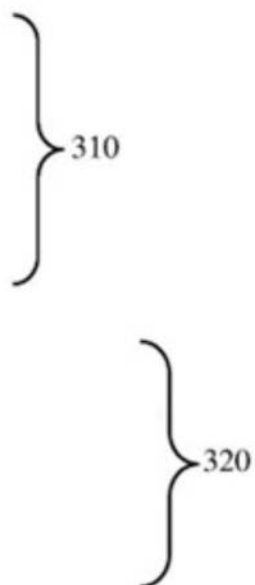
图2

算法 3: 抗量子ECDSA验证 $Verify_q$.

```

1 开始
2   $G \leftarrow$  ECC 基点;  $P \leftarrow$  ECC 次序;
3   $K_p \leftarrow$  ECC 公钥;
4   $R_x, s \leftarrow$  签名  $\sigma$ ;  $\pi \leftarrow$  证明;  $M \leftarrow$  消息;
5  计算  $s^{-1}$  其中  $s * s^{-1} \equiv 1 \bmod P$ ;
6  计算消息的散列值  $H(M)$ ;
7  计算  $u_1 = s^{-1} * H(M) \bmod P$ ;
8  计算  $u_2 = s^{-1} * R_x \bmod P$ ;
9  计算  $V = (V_x, V_y)$  where  $V = u_1 \cdot G + u_2 \cdot K_p \bmod P$ ;
10 如果  $V_x \neq R_x$  则
11  | 返回“签名验证失败”
12 结束
13 否则
14  | 验证ZKBoo证明 $\pi$ =开始
15  | | 检查 $R_x$ 、 $s$ 在证明中是否已提交
16  | | 检查根据未知预映射对 $K_p$ 的零知识计算是否正确;
17  | | 如果检查失败, 则
18  | | | 返回 “签名验证失败”
19  | | 结束
20  | 结束
21 结束
22 返回成功;
23 结束

```



300

图3

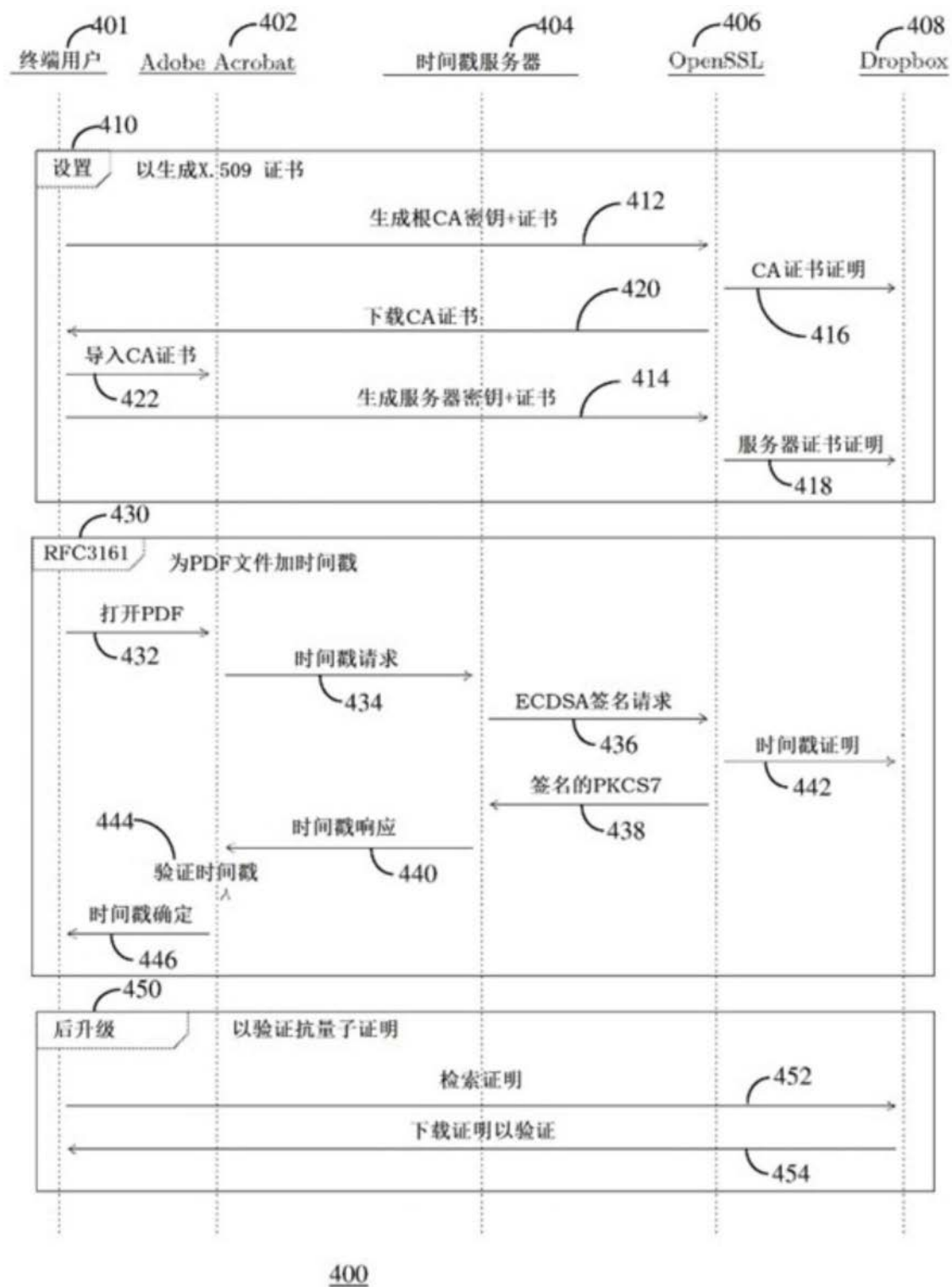


图4

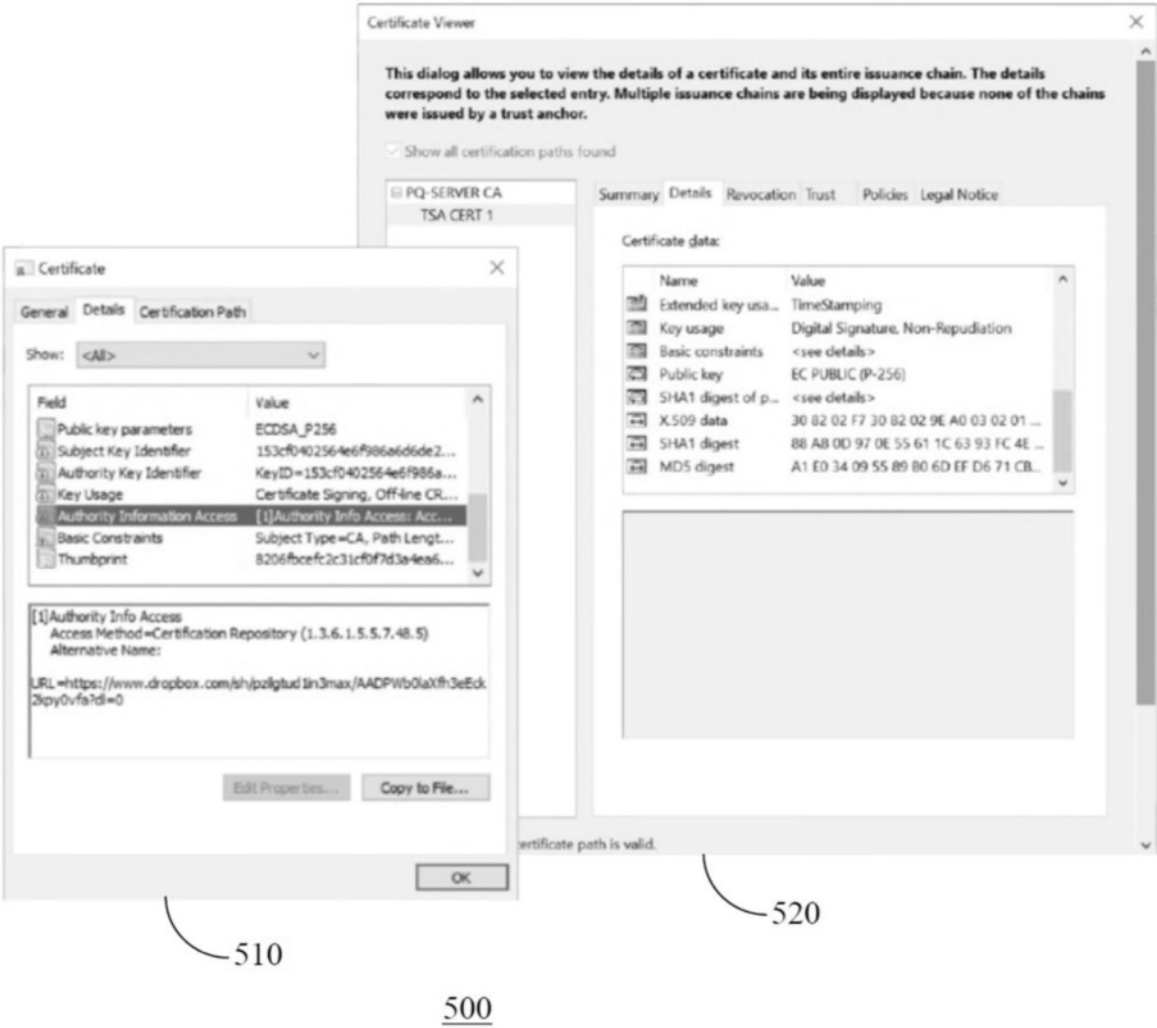
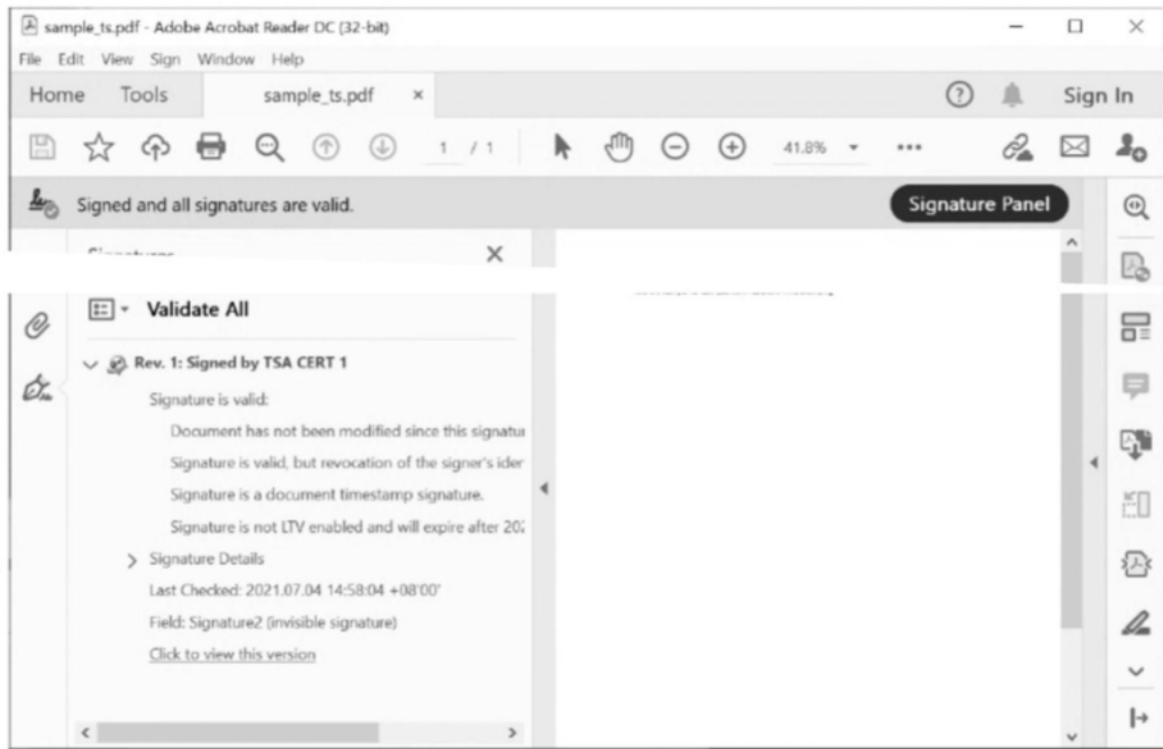


图5



600

图6