(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102223364 A
(43)申请公布日 2011.10.19

(21)申请号 201110118869.2

(22)申请日 2011.05.09

(71)申请人 飞天诚信科技股份有限公司
地址 100085 北京市海淀区学清路 9 号汇智大厦 B 座 17 层

(72)发明人 陆舟 于华章

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/00(2006.01)

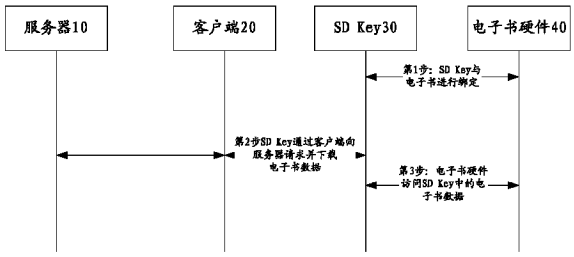
权利要求书 6 页 说明书 18 页 附图 2 页

(54)发明名称

一种访问电子书数据的方法及系统

(57)摘要

本发明提供一种访问电子书数据库的方法，包括：步骤 A：电子书硬件与电子设备建立连接并协商一阅读密钥；步骤 B：电子设备通过客户端下载电子书数据，具体为：首先电子设备与客户端建立连接并；客户端向服务器发送建立连接的请求；服务器通过客户端对电子设备进行身份验证，验证不通过则拒绝访问，验证通过则服务器用下载密钥对电子书数据进行加密并通过客户端将加密后的电子书数据发送给电子设备；步骤 C：电子书硬件与电子设备建立连接，使用下载密钥和/或阅读密钥对加密后的电子书数据进行处理，电子书硬件显示电子书数据。本实施例提供的方法不仅使得电子书的下载和阅读更加快捷，还实现了对电子书版权的保护。



CN 102223364 A

1. 一种访问电子书数据的方法，其特征在于，包括：

步骤 A：电子书硬件与电子设备建立连接并协商一阅读密钥，所述电子设备是具有兼容 SD 卡接口、加解密功能、存储功能的装置；

步骤 B：所述电子设备通过客户端下载电子书数据，具体为：

首先所述电子设备与客户端建立连接；

所述客户端向服务器发送建立连接的请求；

所述服务器通过客户端对所述电子设备进行身份验证，验证不通过则拒绝访问，验证通过则所述服务器用下载密钥对电子书数据进行加密并通过客户端将所述加密后的电子书数据发送给所述电子设备；

步骤 C：所述电子书硬件与所述电子设备建立连接，使用下载密钥和 / 或阅读密钥对加密后的电子书数据进行处理，所述电子书硬件显示所述电子书数据；

其中，所述步骤 A 和步骤 B 的顺序可调换。

2. 如权利要求 1 所述的访问电子书数据的方法，其特征在于，所述电子书硬件与电子设备协商一阅读密钥是电子书硬件中产生阅读密钥并将所述阅读密钥发送给电子设备或电子设备中产生阅读密钥并将所述阅读密钥和 / 或该电子设备的硬件序列号发送给电子书硬件的过程，所述阅读密钥为对称密钥或非对称密钥，当所述阅读密钥为非对称密钥时发送的密钥是非对称密钥的公钥。

3. 如权利要求 2 所述的访问电子书数据的方法，其特征在于，所述电子书硬件中产生阅读密钥为预先设置产生阅读密钥或预先生成产生阅读密钥，电子设备中产生阅读密钥包括预先设置产生阅读密钥或预先生成产生阅读密钥。

4. 如权利要求 3 所述的访问电子书数据的方法，其特征在于，所述阅读密钥为一个对称密钥，所述电子书硬件中产生阅读密钥具体为：在电子书硬件中预先产生一个随机数作为对称密钥。

5. 如权利要求 2 所述的访问电子书数据的方法，其特征在于，所述电子书硬件中或电子设备中产生阅读密钥具体为：所述电子书硬件与电子设备进行连接时，电子书硬件中或电子设备内部产生一个随机数作为对称密钥或产生一非对称密钥。

6. 如权利要求 1 所述的访问电子书数据的方法，其特征在于，所述协商一下载密钥具体为：所述电子设备预先设置或预先随机产生一对称的下载密钥，在进行第一次下载电子书时电子设备会直接通过客户端进行下载并通过客户端将所述下载密钥发送给服务器进行保存，或

所述电子设备预先设置一对称的下载密钥且在所述服务器中预先保存有对应的对称密钥备份。

7. 如权利要求 6 所述的访问电子书数据的方法，其特征在于，所述服务器通过客户端对所述电子设备进行身份验证是采用冲击响应的方法进行的，具体为：

所述服务器产生一个挑战码并将挑战码通过客户端传送给电子设备；

所述电子设备接收到挑战码后，使用下载密钥或下载密钥备份对挑战码进行加密运算，并将加密结果作为响应数据通过客户端回传给服务器；

所述服务器使用下载密钥对所述挑战码进行加密运算，得到认证数据，所述服务器将所述认证数据与所述电子设备回传的响应数据进行比较，并判断比较结果是否一致。

8. 如权利要求 7 所述的访问电子书数据的方法，其特征在于，所述服务器通过客户端向所述电子设备发送用下载密钥加密的电子书数据，具体为：

所述服务器将请求下载的电子书数据用保存的下载密钥或下载密钥备份进行加密，形成电子书的第一密文数据，并将所述第一密文数据通过客户端发送给所述电子设备，所述电子设备将所述第一密文数据进行保存。

9. 如权利要求 8 所述的访问电子书数据的方法，其特征在于，所述电子设备通过客户端下载电子书数据前先与所述电子书硬件协商一阅读密钥，所述电子设备将所述第一密文数据用相应地下载密钥进行解密，生成第二明文数据；并将所述第二明文数据用对称阅读密钥或阅读私钥或阅读公钥再次进行加密，得到第二密文数据，并将所述第二密文数据进行保存。

10. 如权利要求 1 所述的访问电子书数据的方法，其特征在于，所述协商一下载密钥具体为：所述电子设备预先设置一非对称的下载密钥，将所述下载密钥的私钥进行私自保存，且在服务器中预先保存与所述下载私钥匹配的下载公钥备份或所述电子设备第一次通过客户端下载电子书时将所述下载公钥发送给服务器进行保存。

11. 如权利要求 10 所述的访问电子书数据的方法，其特征在于，所述服务器通过客户端对所述电子设备进行身份验证，具体为：

所述服务器接收到所述电子设备发送的建立连接请求以后，产生一随机数，并将所述随机数作为随机密钥发送给所述电子设备；

所述电子设备使用下载私钥对接收到的随机密钥进行签名，再将签名结果作为认证数据通过客户端回传给服务器；

所述服务器使用保存的下载公钥或下载公钥备份和所述产生的随机数验证所述认证数据是否为正确的签名。

12. 如权利要求 11 所述的访问电子书数据的方法，其特征在于，所述服务器通过客户端向电子设备发送用下载密钥加密的电子书数据，具体为：

所述服务器将请求下载的电子书数据用保存的下载公钥或下载公钥备份进行加密，形成电子书的第一密文数据，并将第一密文数据通过客户端发送给所述电子设备，所述电子设备将第一密文数据进行保存。

13. 如权利要求 12 所述的访问电子书数据的方法，其特征在于，所述电子设备通过客户端下载电子书数据前先与所述电子书协商一阅读密钥，所述电子设备将所述第一密文数据用相应地下载私钥进行解密，生成第二明文数据；所述电子设备用对称阅读密钥或阅读私钥或阅读公钥对第二明文数据再次进行加密，得到第二密文数据，并将第二密文数据进行保存。

14. 如权利要求 10 所述的访问电子书数据的方法，其特征在于，所述服务器通过客户端向电子设备发送用下载密钥加密的电子书数据，具体为：

所述服务器产生一随机数作为对称会话密钥，并将所请求下载的电子书数据用所述会话密钥进行加密，形成电子书的第一密文数据；

所述服务器将所述会话密钥用下载公钥或下载公钥备份进行加密，形成加密后的会话密钥；

所述服务器通过客户端将所述第一密文数据和加密后的会话密钥一起发送给电子设

备；

所述电子设备将接收到的所述第一密文数据和加密后的会话密钥进行保存。

15. 如权利要求 14 所述的访问电子书数据的方法，其特征在于，所述会话密钥为“书籍的备案号 + 下载时间”或“书籍的备案号 + 下载次数”或“书籍的备案号 + 下载时间”的散列值或“书籍的备案号 + 下载次数”的散列值。

16. 如权利要求 14 所述的访问电子书数据的方法，其特征在于，所述电子设备通过客户端下载电子书数据前先与所述电子书硬件协商一阅读密钥，所述电子设备将所述加密后的会话密钥用相应地下载私钥进行解密，得到会话密钥，并用得到的会话密钥对接收到的第一密文数据进行解密，得到第二明文数据；

所述电子设备用对称阅读密钥或阅读私钥或阅读公钥对所述第二明文数据进行加密，得到第二密文数据，将所述第二密文数据进行保存。

17. 如权利要求 9、13 或 16 任意一项所述的访问电子书数据的方法，其特征在于，所述步骤 C 具体为：

所述电子书硬件向电子设备发送访问电子书数据的请求，所述电子设备响应所述请求并把第二密文数据发送给电子书硬件或不作响应直接将第二密文数据发送给电子书硬件；

所述电子书硬件使用其与电子设备建立连接时协商的阅读密钥对所述第二密文数据进行解密并显示。

18. 如权利要求 9、13 或 16 任意一项所述的访问电子书数据的方法，其特征在于，所述电子书硬件中预先设置多个阅读密钥，所述步骤 A 具体为：所述电子书硬件与电子设备建立连接，所述电子书硬件从所述多个阅读密钥中选择一个未使用过的阅读密钥发送给所述电子设备，然后再读取所述电子设备的硬件序列号并进行保存，发送给所述电子设备的阅读密钥与所述电子设备的硬件序列号一一对应；

相应地，所述步骤 C 具体为：

所述电子书硬件向电子设备发送访问电子书数据的请求，所述电子设备响应所述请求，所述电子书硬件在接收到所述响应后直接进行读取所述电子设备的硬件序列号，并将读取的电子设备硬件序列号与协商阅读密钥时存储的硬件序列号进行比较并判断是否一致，如果否，则访问失败；

如果是，则所述电子书硬件将所述判断结果发送给所述电子设备，所述电子设备在接收到判断结果后将第二密文数据发送给电子书硬件，所述电子书硬件取得绑定时储存的与所述硬件序列号相对应的阅读密钥，并将所接收到的第二密文数据用所述阅读密钥进行解密得到第二明文数据，所述电子书硬件将所述第二明文数据输出到显示器进行显示。

19. 如权利要求 9、13 或 16 任意一项所述的访问电子书数据的方法，其特征在于，所述电子书硬件中预先设置多个阅读密钥，所述步骤 A 具体为：所述电子书硬件与电子设备建立连接，所述电子书硬件从所述多个阅读密钥中选择一个未使用过的阅读密钥发送给所述电子设备，然后再读取所述电子设备的硬件序列号并进行保存，发送给所述电子设备的阅读密钥与所述电子设备的硬件序列号一一对应；

相应地，所述步骤 C 具体为：

所述电子书硬件向电子设备发送访问电子书数据的请求和协商阅读密钥时保存的硬

件序列号，所述电子设备判断电子书硬件发送过来的硬件序列号与其自身的硬件序列号是否一致，如果一致，则所述电子设备响应所述请求，使用阅读密钥对保存的第二密文数据进行解密得到第二明文数据，并将所述第二明文数据发送给电子书硬件，所述电子书硬件接收到所述第二明文数据并输出到显示器上进行显示；如果不一致则拒绝访问。

20. 如权利要求 8、12 或 14 任意一项所述的访问电子书数据的方法，其特征在于，所述下载密钥和阅读密钥为相同的密钥。

21. 如权利要求 8 所述的访问电子书数据的方法，其特征在于，所述步骤 C 具体为：

所述电子书硬件向电子设备发送访问电子书数据的请求，所述电子设备响应所述请求并把第一密文数据发送给电子书硬件或不作响应直接将第一密文数据发送给电子书硬件；

所述电子书硬件使用其保存的阅读密钥对所述第一密文数据进行解密。

22. 如权利要求 12 所述的访问电子书数据的方法，其特征在于，所述电子书硬件中预先设置多个阅读密钥，所述步骤 A 具体为：所述电子书硬件与电子设备建立连接，所述电子书硬件从所述多个阅读密钥中选择一个未使用过的阅读密钥发送给所述电子设备，然后再读取所述电子设备的硬件序列号并进行保存，发送给所述电子设备的阅读密钥与所述电子设备的硬件序列号一一对应；

相应地，所述步骤 C 具体为：

所述电子书硬件向电子设备发送访问电子书数据的请求和其保存的硬件序列号，所述电子设备判断其自身的硬件序列号与所述电子书硬件发送来的硬件序列号是否一致，如果一致，则所述电子设备响应所述请求并使用与硬件序列号一致的阅读私钥对第一密文数据进行解密，或不作响应直接使用与硬件序列号一致的阅读私钥对第一密文数据进行解密；

如果不一致，则访问失败。

23. 如权利要求 14 所述的访问电子书数据的方法，其特征在于，所述电子书硬件中预先设置多个阅读密钥，所述步骤 A 具体为：所述电子书硬件与电子设备建立连接，所述电子书硬件从所述多个阅读密钥中选择一个未使用过的阅读密钥发送给所述电子设备，然后再读取所述电子设备的硬件序列号并进行保存，发送给所述电子设备的阅读密钥与所述电子设备的硬件序列号一一对应；

相应地，所述步骤 C 具体为：

所述电子书硬件向电子设备发送访问电子书数据的请求和其保存的硬件序列号，所述电子设备判断其自身的硬件序列号与所述电子书硬件发送来的硬件序列号是否一致，如果一致，则所述电子设备响应所述请求并使用与硬件序列号一致的阅读私钥对加密后的会话密钥进行解密得到会话密钥，再用会话密钥对第一加密数据进行解密得到电子书数据；

如果不一致，则访问失败。

24. 一种访问电子书数据的系统，包括服务器、客户端和电子书硬件，其特征在于，还包括电子设备，所述服务器包括：

第一接收模块，用于接收第二发送模块发送的下载密钥；

第一存储模块，用于存储电子书数据和下载密钥；

第一验证模块，用于验证与其进行通讯的客户端上插入的电子设备的身份；

第一执行模块，用于使用第一存储模块中的下载密钥对存储的电子书数据进行加密，

形成第一加密数据；

第一发送模块，用于向所述电子设备发送第一加密数据；

第一总线模块，用于将所述服务器中的各硬件模块进行连接；

所述客户端用于与电子设备进行连接，并用于与所述服务器进行通讯；

所述电子设备具有兼容 SD 卡接口、加解密运算和存储功能的装置，具体包括：

第二接口模块，用于将所述电子设备分别与所述客户端和所述电子书硬件进行连接；

第二接收模块，用于接收所述第一发送模块发送的第一加密数据并进行储存，还用于接收第三发送模块发送的阅读密钥；

第二发生模块，用于产生下载密钥和 / 或阅读密钥，所述下载密钥和 / 或阅读密钥为对称密钥或非对称密钥；

第二执行模块，用于对所述第二接收模块接收到的第一加密数据进行解密，再使用所述第二发生模块中的阅读密钥对解密后的数据进行加密，形成第二密文数据；

第二存储模块，用于存储所述第二执行模块产生的第二加密数据或第二接收模块接收到的第一加密数据，还用于储存所述电子书硬件传送的阅读密钥；

第二解密模块，用于将所述第二存储模块中的密文数据进行解密得到电子书明文数据；

第二发送模块，用于将所述第二解密模块中的明文数据或第二存储模块中的密文数据发送给所述电子书硬件，还用于将所述第二生成模块中的阅读密钥发送给所述电子书硬件，还用于将所述第二发生模块中的下载密钥通过客户端发送给第一接收模块；

第二总线模块，用于将所述电子设备中的各硬件模块进行连接；

所述电子书硬件包括：

第三接口模块，用于将所述电子设备与所述电子书硬件进行连接，所述第三接口模块与第二接口模块连接；

第三访问模块，用于向所述电子设备发送访问电子书数据的请求，所述第三访问模块与第二解密模块连接；

第三接收模块，用于接收所述第二发送模块发送的明文数据或密文数据，还用于接收所述第二发送模块发送的阅读密钥；

第三发生模块，用于产生对称阅读密钥或非对称阅读密钥；

第三存储模块，用于存储所述第三接收模块接收的阅读密钥，或用于存储所述第三发生模块产生的所述阅读密钥；

第三发送模块，用于将所述第三发生模块产生的阅读密钥发送给所述第二接收模块；

第三执行模块，用于将所述第三接收模块中的密文数据用所述第三存储模块中的阅读密钥进行解密，得到明文数据；

第三总线模块，用于将所述电子书硬件中的各模块进行连接。

25. 如权利要求 24 所述的访问电子书数据的系统，其特征在于，所述服务器还包括第一发生模块，其用于产生一个挑战码并将挑战码传送给电子设备；

所述第二执行模块还用于使用所述第二发生模块产生的下载密钥对所述挑战码进行加密运算，并将加密结果作为响应数据回传给第一验证模块；

所述第一验证模块使用第一存储模块中的下载密钥对所述挑战码进行加密运算，得到

认证数据，所述第一验证模块将所述认证数据与所述第二执行模块回传的响应数据进行比较，并判断比较结果是否一致。

26. 如权利要求 24 所述的访问电子书数据的系统，其特征在于，所述服务器还包括第一发生模块，其用于产生一随机数，并将所述随机数作为随机密钥发送给所述第二执行模块；

所述第二执行模块还用于使用所述第二发生模块产生的下载私钥对接收到的随机密钥进行签名，再将签名结果作为认证数据回传给所述服务器的第一验证模块；

所述服务器的第一验证模块使用第一存储模块中的下载公钥和所述随机数验证所述认证数据是否为正确的签名。

27. 如权利要求 26 所述的访问电子书数据的系统，其特征在于，所述会话密钥为“书籍的备案号 + 下载时间”或“书籍的备案号 + 下载次数”或“书籍的备案号 + 下载时间”的散列值或“书籍的备案号 + 下载次数”的散列值。

28. 如权利要求 24 所述的访问电子书数据的系统，其特征在于，所述服务器还包括第一发生模块，其用于产生一随机数作为对称会话密钥；

所述第一执行模块还可用于将所述电子书数据用所述会话密钥进行加密，形成第一密文数据，第一执行模块还用于将所述会话密钥用下载公钥进行加密，形成加密后的会话密钥；

所述第一发送模块将所述第一密文数据和加密后的会话密钥一起发送给所述第二接收模块。

29. 如权利要求 28 所述的访问电子书数据的系统，其特征在于，所述第二执行模块用于对所述第二接收模块接收到的第一加密数据进行解密，再使用所述第二发生模块中的阅读密钥对解密后的数据进行加密，形成第二密文数据，具体为：

所述第二执行模块使用第二发生模块所产生的下载密钥对所述第二接收模块接收到的加密后的会话密钥进行解密，得到会话密钥，再用得到的会话密钥对所述第二接收模块中的所述第一密文数据进行解密得到第二明文数据，所述第二执行模块使用第二发生模块产生的阅读密钥或第二接收模块接收到的阅读密钥对所述第二明文数据进行加密，得到第二密文数据。

30. 如权利要求 24 所述的访问电子书数据的系统，其特征在于，所述第三发生模块中产生的阅读密钥是事先预置得到或随机产生得到，所述阅读密钥为对称密钥或非对称密钥。

31. 如权利要求 24 所述的访问电子书数据的系统，其特征在于，所述第三访问模块还用于读取所述电子设备的硬件序列号。

一种访问电子书数据的方法及系统

技术领域

[0001] 本发明涉及信息安全领域，特别涉及一种访问电子书数据的方法及系统。

背景技术

[0002] 一般传统书籍体积大而且携带不方便，再加上不易长久收藏，故出现一种新型态的电子书（eBook）阅读方式，电子书是将书籍内容一页一页显示于一电子装置平台（如计算机、掌上型计算机、PDA、电子书阅读器等）的屏幕，此种阅读方式使电子书以电子文件方式存储于电子装置平台，而更容易长期的收藏和保管，使用者在外出时只需携带一台掌上型计算机、PDA 或电子书阅读器搭配阅读软件，借由插接存有电子书数据的记忆卡即可阅读，非常快捷和方便。

[0003] 而为了新增电子书的内容，一般均通过上网方式下载电子书，使用者需要自行拔接上网，并连接至下载电子书的服务器网站，再由使用者本身根据个人爱好来下载自己所需要的电子书数据，但是市面上也存在越来越多的盗版书籍，随着互联网的迅速发展，电子图书出版的版权问题越来越受到人们的关注。由于网络快捷的传播方式和广泛的用户群体，电子图书出版中的侵权行为经常发生，电子图书版权保护问题便尖锐地摆到人们的议事日程上来。探讨电子图书侵权行为的特点，积极寻找应对策略，对于出版单位持续健康地开展数字出版业务具有相当重要的现实意义。

发明内容

[0004] 本发明基于现有技术的不足，提供了一种访问电子书数据的方法及系统，不仅使得电子书的下载和阅读更加快捷，还实现了对电子书版权的保护。

[0005] 本发明提供了一种访问电子书数据的方法，具体包括：

[0006] 步骤 A：电子书硬件与电子设备建立连接并协商一阅读密钥，所述电子设备是具有兼容 SD 卡接口、加解密功能、存储功能的装置；

[0007] 步骤 B：所述电子设备通过客户端下载电子书数据，具体为：

[0008] 首先所述电子设备与客户端建立连接；

[0009] 所述客户端向服务器发送建立连接的请求；

[0010] 所述服务器通过客户端对所述电子设备进行身份验证，验证不通过则拒绝访问，验证通过则所述服务器用下载密钥对电子书数据进行加密并通过客户端将所述加密后的电子书数据发送给所述电子设备；

[0011] 步骤 C：所述电子书硬件与所述电子设备建立连接，使用下载密钥和 / 或阅读密钥对加密后的电子书数据进行处理，所述电子书硬件显示所述电子书数据；

[0012] 其中，所述步骤 A 和步骤 B 的顺序可调换。

[0013] 所述电子书硬件与电子设备协商一阅读密钥是电子书硬件中产生阅读密钥并将所述阅读密钥发送给电子设备或电子设备中产生阅读密钥并将所述阅读密钥和 / 或该电子设备的硬件序列号发送给电子书硬件的过程，所述阅读密钥为对称密钥或非对称密钥，

当所述阅读密钥为非对称密钥时发送的密钥是非对称密钥的公钥。

[0014] 所述电子书硬件中产生阅读密钥为预先设置产生阅读密钥或预先生成产生阅读密钥，电子设备中产生阅读密钥包括预先设置产生阅读密钥或预先生成产生阅读密钥。

[0015] 所述阅读密钥为一个对称密钥，所述电子书硬件中产生阅读密钥具体为：在电子书硬件中预先产生一个随机数作为对称密钥。

[0016] 所述电子书硬件中或电子设备中产生阅读密钥具体为：所述电子书硬件与电子设备进行连接时，电子书硬件中或电子设备内部产生一个随机数作为对称密钥或产生一非对称密钥。

[0017] 所述协商一下载密钥具体为：所述电子设备预先设置或预先随机产生一对称的下载密钥，在进行第一次下载电子书时电子设备会直接通过客户端进行下载并通过客户端将所述下载密钥发送给服务器进行保存，或

[0018] 所述电子设备预先设置一对称的下载密钥且在所述服务器中预先保存有对应的对称密钥备份。

[0019] 所述服务器通过客户端对所述电子设备进行身份验证是采用冲击响应的方法进行的，具体为：

[0020] 所述服务器产生一个挑战码并将挑战码通过客户端传送给电子设备；

[0021] 所述电子设备接收到挑战码后，使用下载密钥或下载密钥备份对挑战码进行加密运算，并将加密结果作为响应数据通过客户端回传给服务器；

[0022] 所述服务器使用下载密钥对所述挑战码进行加密运算，得到认证数据，所述服务器将所述认证数据与所述电子设备回传的响应数据进行比较，并判断比较结果是否一致。

[0023] 所述服务器通过客户端向所述电子设备发送用下载密钥加密的电子书数据，具体为：

[0024] 所述服务器将请求下载的电子书数据用保存的下载密钥或下载密钥备份进行加密，形成电子书的第一密文数据，并将所述第一密文数据通过客户端发送给所述电子设备，所述电子设备将所述第一密文数据进行保存。

[0025] 所述电子设备通过客户端下载电子书数据前先与所述电子书硬件协商一阅读密钥，所述电子设备将所述第一密文数据用相应地下载密钥进行解密，生成第二明文数据；并将所述第二明文数据用对称阅读密钥或阅读私钥或阅读公钥再次进行加密，得到第二密文数据，并将所述第二密文数据进行保存。

[0026] 所述协商一下载密钥具体为：所述电子设备预先设置一非对称的下载密钥，将所述下载密钥的私钥进行私自保存，且在服务器中预先保存与所述下载私钥匹配的下载公钥备份或所述电子设备第一次通过客户端下载电子书时将所述下载公钥发送给服务器进行保存。

[0027] 所述服务器通过客户端对所述电子设备进行身份验证，具体为：

[0028] 所述服务器接收到所述电子设备发送的建立连接请求以后，产生一随机数，并将所述随机数作为随机密钥发送给所述电子设备；

[0029] 所述电子设备使用下载私钥对接收到的随机密钥进行签名，再将签名结果作为认证数据通过客户端回传给服务器；

[0030] 所述服务器使用保存的下载公钥或下载公钥备份和所述产生的随机数验证所述

认证数据是否为正确的签名。

[0031] 所述服务器通过客户端向电子设备发送用下载密钥加密的电子书数据，具体为：

[0032] 所述服务器将请求下载的电子书数据用保存的下载公钥或下载公钥备份进行加密，形成电子书的第一密文数据，并将第一密文数据通过客户端发送给所述电子设备，所述电子设备将第一密文数据进行保存。

[0033] 所述电子设备通过客户端下载电子书数据前先与所述电子书协商一阅读密钥，所述电子设备将所述第一密文数据用相应地下载私钥进行解密，生成第二明文数据；所述电子设备用对称阅读密钥或阅读私钥或阅读公钥对第二明文数据再次进行加密，得到第二密文数据，并将第二密文数据进行保存。

[0034] 所述服务器通过客户端向电子设备发送用下载密钥加密的电子书数据，具体为：

[0035] 所述服务器产生一随机数作为对称会话密钥，并将所请求下载的电子书数据用所述会话密钥进行加密，形成电子书的第一密文数据；

[0036] 所述服务器将所述会话密钥用下载公钥或下载公钥备份进行加密，形成加密后的会话密钥；

[0037] 所述服务器通过客户端将所述第一密文数据和加密后的会话密钥一起发送给电子设备；

[0038] 所述电子设备将接收到的所述第一密文数据和加密后的会话密钥进行保存。

[0039] 所述会话密钥为“书籍的备案号 + 下载时间”或“书籍的备案号 + 下载次数”或“书籍的备案号 + 下载时间”的散列值或“书籍的备案号 + 下载次数”的散列值。

[0040] 所述电子设备通过客户端下载电子书数据前先与所述电子书硬件协商一阅读密钥，所述电子设备将所述加密后的会话密钥用相应地下载私钥进行解密，得到会话密钥，并用得到的会话密钥对接收到的第一密文数据进行解密，得到第二明文数据；

[0041] 所述电子设备用对称阅读密钥或阅读私钥或阅读公钥对所述第二明文数据进行加密，得到第二密文数据，将所述第二密文数据进行保存。

[0042] 所述步骤 C 具体为：

[0043] 所述电子书硬件向电子设备发送访问电子书数据的请求，所述电子设备响应所述请求并把第二密文数据发送给电子书硬件或不作响应直接将第二密文数据发送给电子书硬件；

[0044] 所述电子书硬件使用其与电子设备建立连接时协商的阅读密钥对所述第二密文数据进行解密并显示。

[0045] 所述电子书硬件中预先设置多个阅读密钥，所述步骤 A 具体为：所述电子书硬件与电子设备建立连接，所述电子书硬件从所述多个阅读密钥中选择一个未使用过的阅读密钥发送给所述电子设备，然后再读取所述电子设备的硬件序列号并进行保存，发送给所述电子设备的阅读密钥与所述电子设备的硬件序列号一一对应；

[0046] 相应地，所述步骤 C 具体为：

[0047] 所述电子书硬件向电子设备发送访问电子书数据的请求，所述电子设备响应所述请求，所述电子书硬件在接收到所述响应后直接进行读取所述电子设备的硬件序列号，并将读取的电子设备硬件序列号与协商阅读密钥时存储的硬件序列号进行比较并判断是否一致，如果否，则访问失败；

[0048] 如果是，则所述电子书硬件将所述判断结果发送给所述电子设备，所述电子设备在接收到判断结果后将第二密文数据发送给电子书硬件，所述电子书硬件取得绑定时储存的与所述硬件序列号相对应的阅读密钥，并将所接收到的第二密文数据用所述阅读密钥进行解密得到第二明文数据，所述电子书硬件将所述第二明文数据输出到显示器进行显示。

[0049] 所述电子书硬件中预先设置多个阅读密钥，所述步骤 A 具体为：所述电子书硬件与电子设备建立连接，所述电子书硬件从所述多个阅读密钥中选择一个未使用过的阅读密钥发送给所述电子设备，然后再读取所述电子设备的硬件序列号并进行保存，发送给所述电子设备的阅读密钥与所述电子设备的硬件序列号一一对应；

[0050] 相应地，所述步骤 C 具体为：

[0051] 所述电子书硬件向电子设备发送访问电子书数据的请求和协商阅读密钥时保存的硬件序列号，所述电子设备判断电子书硬件发送过来的硬件序列号与其自身的硬件序列号是否一致，如果一致，则所述电子设备响应所述请求，使用阅读密钥对保存的第二密文数据进行解密得到第二明文数据，并将所述第二明文数据发送给电子书硬件，所述电子书硬件接收到所述第二明文数据并输出到显示器上进行显示；如果不一致则拒绝访问。

[0052] 所述下载密钥和阅读密钥为相同的密钥。

[0053] 所述步骤 C 具体为：

[0054] 所述电子书硬件向电子设备发送访问电子书数据的请求，所述电子设备响应所述请求并把第一密文数据发送给电子书硬件或不作响应直接将第一密文数据发送给电子书硬件；

[0055] 所述电子书硬件使用其保存的阅读密钥对所述第一密文数据进行解密。

[0056] 所述电子书硬件中预先设置多个阅读密钥，所述步骤 A 具体为：所述电子书硬件与电子设备建立连接，所述电子书硬件从所述多个阅读密钥中选择一个未使用过的阅读密钥发送给所述电子设备，然后再读取所述电子设备的硬件序列号并进行保存，发送给所述电子设备的阅读密钥与所述电子设备的硬件序列号一一对应；

[0057] 相应地，所述步骤 C 具体为：

[0058] 所述电子书硬件向电子设备发送访问电子书数据的请求和其保存的硬件序列号，所述电子设备判断其自身的硬件序列号与所述电子书硬件发送来的硬件序列号是否一致，如果一致，则所述电子设备响应所述请求并使用与硬件序列号一致的阅读私钥对第一密文数据进行解密，或不作响应直接使用与硬件序列号一致的阅读私钥对第一密文数据进行解密；

[0059] 如果不一致，则访问失败。

[0060] 所述电子书硬件中预先设置多个阅读密钥，所述步骤 A 具体为：所述电子书硬件与电子设备建立连接，所述电子书硬件从所述多个阅读密钥中选择一个未使用过的阅读密钥发送给所述电子设备，然后再读取所述电子设备的硬件序列号并进行保存，发送给所述电子设备的阅读密钥与所述电子设备的硬件序列号一一对应；

[0061] 相应地，所述步骤 C 具体为：

[0062] 所述电子书硬件向电子设备发送访问电子书数据的请求和其保存的硬件序列号，所述电子设备判断其自身的硬件序列号与所述电子书硬件发送来的硬件序列号是否一致，如果一致，则所述电子设备响应所述请求并使用与硬件序列号一致的阅读私钥对加密后的

会话密钥进行解密得到会话密钥，再用会话密钥对第一加密数据进行解密得到电子书数据；

[0063] 如果不一致，则访问失败。

[0064] 一种访问电子书数据的系统，包括服务器、客户端和电子书硬件，还包括电子设备，所述服务器包括：

[0065] 第一接收模块，用于接收第二发送模块发送的下载密钥；

[0066] 第一存储模块，用于存储电子书数据和下载密钥；

[0067] 第一验证模块，用于验证与其进行通讯的客户端上插入的电子设备的身份；

[0068] 第一执行模块，用于使用第一存储模块中的下载密钥对存储的电子书数据进行加密，形成第一加密数据；

[0069] 第一发送模块，用于向所述电子设备发送第一加密数据；

[0070] 第一总线模块，用于将所述服务器中的各硬件模块进行连接；

[0071] 所述客户端用于与电子设备进行连接，并用于与所述服务器进行通讯；

[0072] 所述电子设备具有兼容 SD 卡接口、加解密运算和存储功能的装置，具体包括：

[0073] 第二接口模块，用于将所述电子设备分别与所述客户端和所述电子书硬件进行连接；

[0074] 第二接收模块，用于接收所述第一发送模块发送的第一加密数据并进行储存，还用于接收第三发送模块发送的阅读密钥；

[0075] 第二发生模块，用于产生下载密钥和 / 或阅读密钥，所述下载密钥和 / 或阅读密钥为对称密钥或非对称密钥；

[0076] 第二执行模块，用于对所述第二接收模块接收到的第一加密数据进行解密，再使用所述第二发生模块中的阅读密钥对解密后的数据进行加密，形成第二密文数据；

[0077] 第二存储模块，用于存储所述第二执行模块产生的第二加密数据或第二接收模块接收到的第一加密数据，还用于储存所述电子书硬件传送的阅读密钥；

[0078] 第二解密模块，用于将所述第二存储模块中的密文数据进行解密得到电子书明文数据；

[0079] 第二发送模块，用于将所述第二解密模块中的明文数据或第二存储模块中的密文数据发送给所述电子书硬件，还用于将所述第二生成模块中的阅读密钥发送给所述电子书硬件，还用于将所述第二发生模块中的下载密钥通过客户端发送给第一接收模块；

[0080] 第二总线模块，用于将所述电子设备中的各硬件模块进行连接；

[0081] 所述电子书硬件包括：

[0082] 第三接口模块，用于将所述电子设备与所述电子书硬件进行连接，所述第三接口模块与第二接口模块连接；

[0083] 第三访问模块，用于向所述电子设备发送访问电子书数据的请求，所述第三访问模块与第二解密模块连接；

[0084] 第三接收模块，用于接收所述第二发送模块发送的明文数据或密文数据，还用于接收所述第二发送模块发送的阅读密钥；

[0085] 第三发生模块，用于产生对称阅读密钥或非对称阅读密钥；

[0086] 第三存储模块，用于存储所述第三接收模块接收的阅读密钥，或用于存储所述第

三发生模块产生的所述阅读密钥；

[0087] 第三发送模块，用于将所述第三发生模块产生的阅读密钥发送给所述第二接收模块；

[0088] 第三执行模块，用于将所述第三接收模块中的密文数据用所述第三存储模块中的阅读密钥进行解密，得到明文数据；

[0089] 第三总线模块，用于将所述电子书硬件中的各模块进行连接。

[0090] 所述服务器还包括第一发生模块，其用于产生一个挑战码并将挑战码传送给电子设备；

[0091] 所述第二执行模块还用于使用所述第二发生模块产生的下载密钥对所述挑战码进行加密运算，并将加密结果作为响应数据回传给第一验证模块；

[0092] 所述第一验证模块使用第一存储模块中的下载密钥对所述挑战码进行加密运算，得到认证数据，所述第一验证模块将所述认证数据与所述第二执行模块回传的响应数据进行比较，并判断比较结果是否一致。

[0093] 所述服务器还包括第一发生模块，其用于产生一随机数，并将所述随机数作为随机密钥发送给所述第二执行模块；

[0094] 所述第二执行模块还用于使用所述第二发生模块产生的下载私钥对接收到的随机密钥进行签名，再将签名结果作为认证数据回传给所述服务器的第一验证模块；

[0095] 所述服务器的第一验证模块使用第一存储模块中的下载公钥和所述随机数验证所述认证数据是否为正确的签名。

[0096] 所述会话密钥为“书籍的备案号 + 下载时间”或“书籍的备案号 + 下载次数”或“书籍的备案号 + 下载时间”的散列值或“书籍的备案号 + 下载次数”的散列值。

[0097] 所述服务器还包括第一发生模块，其用于产生一随机数作为对称会话密钥；

[0098] 所述第一执行模块还可用于将所述电子书数据用所述会话密钥进行加密，形成第一密文数据，第一执行模块还用于将所述会话密钥用下载公钥进行加密，形成加密后的会话密钥；

[0099] 所述第一发送模块将所述第一密文数据和加密后的会话密钥一起发送给所述第二接收模块。

[0100] 所述第二执行模块用于对所述第二接收模块接收到的第一加密数据进行解密，再使用所述第二发生模块中的阅读密钥对解密后的数据进行加密，形成第二密文数据，具体为：

[0101] 所述第二执行模块使用第二发生模块所产生的下载密钥对所述第二接收模块接收到的加密后的会话密钥进行解密，得到会话密钥，再用得到的会话密钥对所述第二接收模块中的所述第一密文数据进行解密得到第二明文数据，所述第二执行模块使用第二发生模块产生的阅读密钥或第二接收模块接收到的阅读密钥对所述第二明文数据进行加密，得到第二密文数据。

[0102] 所述第三发生模块中产生的阅读密钥是事先预置得到或随机产生得到，所述阅读密钥为对称密钥或非对称密钥。

[0103] 所述第三访问模块还用于读取所述电子设备的硬件序列号。

[0104] 本发明通过SD Key来通过客户端向服务器申请下载电子书数据，并存储下载后的

电子书数据，电子书硬件访问电子书数据之前需与 SD Key 进行有效的绑定连接，方可访问电子书，否则将无法访问电子书数据，电子书数据存储在 SD Key 内，增加了电子书数据的安全性，不仅使得电子书的下载和阅读更加快捷，还实现了对电子书版权的保护。

附图说明

[0105] 图 1 为本实施例提供的一种访问电子书数据的总体方法流程图；

[0106] 图 2 为本实施例提供的 SD Key 通过客户端下载电子书数据的方法图；

[0107] 图 3 为本实施例提供的一种访问电子书数据的系统图。

具体实施方式

[0108] 本实施例提供了一种访问电子书数据的方法及系统，具体涉及服务器 10、客户端 20、SD Key30 和电子书硬件 40。为使发明内容更加清晰，下面结合实施例和附图来对本发明做进一步说明，但不作为对本发明的限定。

[0109] 实施例 1

[0110] 参见图 1，为本实施例 1 提供的一种访问电子书数据的总体方法流程图，具体为：

[0111] 第 1 步：电子书硬件与 SD Key 进行绑定；

[0112] 优选的，SD Key 是具有标准 SD 卡接口的信息安全设备，同时具有加解密和存储的功能，可以通过其 API 接口实现对加密锁的访问，加密硬件支持 512/1024/2048 位 RSA、DES、3DES、SHA1、HMAC、MD5 算法，兼容 SD 卡接口的设备有 TF 卡、MMC 卡、MINI-MMC 卡等。

[0113] 本实施例中，SD Key 与电子书进行绑定以后才可以进行数据的通信。

[0114] 具体为，电子书硬件与 SD Key 进行连接，绑定的过程就是电子书硬件向 SDKey 发送密钥，或 SD Key 向电子书硬件发送密钥或密钥和 SD Key 硬件序列号或 SD Key 向电子书硬件发送密钥和电子书硬件读取 SD Key 硬件序列号的过程，确保 SD Key 中的电子书数据能够正常的被电子书硬件访问；

[0115] 需要说明的是，上述密钥为阅读密钥，该阅读密钥可以是对称阅读密钥也可以是非对称阅读密钥，上述绑定过程所发送的是对称阅读密钥或阅读公钥，阅读私钥则保存在 SD Key 或电子书硬件内不得导出。

[0116] 第 2 步：SD Key 通过客户端向服务器请求并下载电子书数据；

[0117] 具体为，

[0118] SD Key 与客户端主机进行连接；

[0119] 优选的，客户端接收用户发送的下载电子书数据的请求，客户端响应请求并向服务器发送下载电子书数据的请求并和服务器建立连接；本实施例中所述的客户端用于 SD Key 和服务器之间的连接和通信，可以是用户 PC 机、上网本、带有上网功能的浏览器、带有上网功能的电纸书或者手机等。

[0120] 服务器通过客户端对 SD Key 进行身份验证，并判断验证是否通过；

[0121] 如果是，服务器则将电子书明文数据进行加密后的第一密文数据通过客户端发送给 SD Key，SD Key 将接收到的第一密文数据进行存储；或所述服务器则将加密后的第一密文数据通过客户端发送给 SD Key，SD Key 将接收到的第一密文数据用存储的与服务器加密电子书数据相匹配的下载密钥进行解密，得到第二明文数据，并用存储的阅读密钥对明文

数据进行再次加密，得到第二密文数据并进行存储；

[0122] 如果否，服务器则拒绝客户端的请求；

[0123] 需要说明的是，下载的过程由下载密钥对电子书明文数据进行加密以后得到电子书密文数据，如果下载密钥是对称密钥，则用对称密钥对电子书明文数据进行加密形成电子书密文数据；如果下载密钥是非对称密钥，则用非对称公钥对电子书明文数据进行加密形成电子书密文数据。

[0124] 第 3 步：电子书硬件访问 SD Key 中的电子书数据；

[0125] 具体的，电子书硬件与 SD Key 进行连接，电子书硬件用对称密钥或非对称密钥的公钥或非对称密钥的私钥对 SD Key 中存储的电子书数据进行解密并访问；

[0126] 如果密钥匹配，则解密成功，可以正常显示电子书数据；

[0127] 如果密钥不匹配，则解密失败，不可以正常显示电子书数据。

[0128] 或；

[0129] SD Key 用自身的对称密钥或非对称密钥的私钥对电子书密文数据进行解密，得到明文数据，再将明文数据传送给电子书硬件，电子书硬件显示电子书数据。

[0130] 在本实施例中，客户端向服务器发送下载电子书数据的请求，请求成功后服务器将电子书数据发送给 SD Key 的过程中，如果被访问的电子书数据为第一密文数据，上述实施例的第 1 步和第 2 步可以互换顺序；如果被访问的电子书数据为第二密文数据，上述实施例的第 1 步和第 2 步则不可以互换顺序。

[0131] 实施例 2

[0132] 本实施例 2 提供了实施例 1 的第 1 步中电子书硬件与 SD Key 进行绑定的具体方法，但不作为对本发明的限定。

[0133] 如下为本实施例 2 提供的电子书硬件与 SD Key 绑定的第一种方法，具体为：

[0134] 优选的，

[0135] 步骤 101：电子书硬件中产生一个随机数作为对称密钥，本方法称为对称阅读密钥，每个电子书内的阅读密钥是不同且唯一的；

[0136] 或，

[0137] 电子书硬件中产生一非对称密钥，本方法称为非对称阅读密钥，每个电子书硬件内的阅读密钥是不同且唯一的，阅读私钥不可导出；

[0138] 或，

[0139] 电子书硬件内预置了一对称密钥，本方法称之为对称阅读密钥，每个电子书硬件内的阅读密钥是不同且唯一的；

[0140] 或，

[0141] 电子书硬件内预置了一非对称密钥，本方法称之为非对称阅读密钥，每个电子书硬件内的阅读密钥是不同且唯一的，阅读私钥不可导出；

[0142] 或，

[0143] 电子书硬件与 SD Key 建立绑定连接时，电子书硬件内部产生一个随机数作为对称密钥，本方法称之为对称阅读密钥，每个电子书内的阅读密钥是不同且唯一的；

[0144] 或，

[0145] 电子书硬件与 SD Key 建立绑定连接时，电子书硬件内部产生一个非对称密钥，本

方法称之为非对称阅读密钥，每个电子书内的阅读密钥是不同且唯一的，阅读私钥不可导出；

[0146] 步骤 102：电子书硬件与 SD Key 建立连接，电子书硬件将对称阅读密钥或阅读公钥发送到 SD Key 中，SD Key 将此阅读公钥保存在存储区域内。

[0147] 如下为本实施例提供的电子书硬件与 SD Key 进行绑定的第二种方法，具体为：

[0148] 步骤 201：电子书硬件内预置了多个对称密钥，本方法称之为对称阅读密钥，电子书内的每个阅读密钥是不同且唯一的；

[0149] 或，

[0150] 电子书硬件内预置了多个非对称密钥，本方法称之为非对称阅读密钥，电子书内的每个阅读密钥是不同且唯一的，阅读私钥不可导出；

[0151] 步骤 202：电子书硬件与 SD Key 建立连接，电子书硬件将选择多个阅读密钥中没有进行绑定的一个阅读密钥，并将对称阅读密钥或阅读公钥发送到 SD Key 中，SD Key 将对称阅读密钥或阅读公钥保存在存储区域内，电子书硬件读取当前 SD Key 的硬件序列号或 SD Key 将自身的硬件序列号发送给电子书硬件，电子书硬件将 SD Key 硬件序列号保存到存储区域内；

[0152] 需要说明的是，SD Key 的硬件序列号与该阅读密钥是相对应的；

[0153] 还需要说明的是，电子书硬件内部产生的对称密钥可以是由随机数发生器来产生的随机数，该随机数可作为对称密钥；电子书硬件内部产生的非对称密钥可以是由非对称密钥协处理器经过非对称算法产生的。

[0154] 如下为本实施例提供的电子书硬件与 SD Key 进行绑定的第三种方法，具体为：

[0155] 步骤 301：电子书硬件与 SD Key 连接时，SD Key 内部产生一个随机数作为对称密钥，本方法称之为对称阅读密钥，每个电子书内的阅读密钥是不同且唯一的；

[0156] 或，

[0157] 电子书硬件与 SD Key 建立连接时，SD Key 内部产生一个非对称密钥，本方法称之为非对称阅读密钥，每个电子书内的阅读密钥是不同且唯一的，阅读私钥不可导出；

[0158] 或，

[0159] SD Key 内预置一个对称密钥，本方法称之为对称阅读密钥，电子书内的每个阅读密钥是不同且唯一的；

[0160] 或，

[0161] SD Key 内预置一个非对称密钥，本方法称之为非对称阅读密钥，电子书内的每个阅读密钥是不同且唯一的，阅读私钥不可导出；

[0162] 步骤 302：电子书硬件与 SD Key 绑定时，SD Key 将对称阅读密钥或阅读公钥发送到电子书硬件中，电子书硬件读取当前 SD Key 的硬件序列号或 SD Key 将自身的硬件序列号发送给电子书硬件，电子书硬件将 SD Key 发送的对称阅读密钥或阅读公钥和 SD Key 的硬件序列号保存到存储区域内。

[0163] 本实施例所述的以上方法中，对称阅读密钥和非对称阅读密钥统称为阅读密钥，所述阅读公钥所指的是非对称阅读密钥的公钥，所述阅读私钥所指的是非对称阅读密钥的私钥。

[0164] 需要说明的是，SD Key 内部产生的对称密钥可以是由随机数发生器来产生的随机

数，该随机数可作为对称密钥；SD Key 内部产生的非对称密钥可以是由非对称密钥协处理器经过非对称算法产生的。

[0165] 实施例 3

[0166] 本实施例 3 提供了实施例 1 的第 2 步中 SD Key 通过客户端下载电子书数据的具体方法，下面结合附图和具体实施例来对本发明做进一步说明，但不作为对本发明的限定。

[0167] 参见图 2，为本实施例 3 提供的 SD Key 通过客户端下载电子书数据的方法图；

[0168] 如下为本实施例 3 提供的 SD Key 通过客户端下载电子书数据的第一种方法，具体为：

[0169] 步骤 401：SD Key 与客户端主机建立连接；

[0170] 步骤 402：客户端向服务器发送建立连接的请求；

[0171] 优选的，SD Key 的安全区域中预置一对称密钥，本方法称为对称下载密钥，与其对应的服务器数据库中事先已保存有对称下载密钥的备份，该对称下载密钥保存在 SD Key 安全区域内，不能导出 SD Key 外；或 SD Key 的安全区域中预置一对称密钥，本方法称为对称下载密钥，在第一次下载时，客户端将 SD Key 中的对称下载密钥传送给服务器，服务器将对称下载密钥保存在数据库中；或在第一次下载时，SD Key 产生一个随机数作为对称密钥，本方法称为对称下载密钥，客户端将 SD Key 中的对称下载密钥传送给服务器，服务器将对称下载密钥保存在数据库中；

[0172] 步骤 403：服务器通过客户端对 SD Key 进行验证并判断验证是否通过；

[0173] 具体的，服务器接收到客户端发出的建立连接请求后，对 SD Key 采取冲击响应的验证方法进行身份验证，并判断验证是否通过；

[0174] 所述冲击响应的验证方法具体为，

[0175] 服务器随机生产一个挑战码并将挑战码通过客户端传送给 SD Key，挑战码可以是一串数字、字母和 / 或符号的组合；例如，挑战码可以采用 64 位的二进制数；

[0176] SD Key 接收到挑战码以后，使用预置在 SD Key 中的对称下载密钥对挑战码进行对称加密运算得到一个结果，客户端将结果作为响应数据传给服务器；

[0177] 在服务器端，使用存储在服务器数据库中的 SD Key 对称下载密钥备份或第一次下载时客户端传送给服务器的对称下载密钥对该挑战码进行 3DES 加密运算，得到认证数据，服务器将认证数据与客户端传回的响应数据进行比较，并判断比较结果是否一致；

[0178] 如果是，SD Key 通过客户端与服务器建立连接成功，客户端通过网页 Act iveX 控件技术或运行在客户端的程序访问 SD Key，继续执行步骤 404；

[0179] 如果否，服务器则拒绝客户端的请求。

[0180] 步骤 404：服务器向客户端发送建立连接成功的响应并通过客户端向 SD Key 发送电子书数据；

[0181] 具体为，

[0182] 步骤 404-1：服务器将所请求下载的电子书数据用服务器数据库中备份的对称下载密钥或第一次下载时客户端传送给服务器的对称下载密钥进行加密，形成电子书的第一密文数据，并将第一密文数据通过客户端发送给 SD Key；

[0183] 步骤 404-2：SD Key 将接收到的第一密文数据保存在存储区域内；

[0184] 以上的方法是客户端下载电子书数据的下载密钥和电子书硬件访问电子书数据

的阅读密钥采用同一对称密钥的方法；为增加对电子书数据的保护，以上下载密钥和阅读密钥可采用不同的对称密钥，其中上述步骤 404 还可以替代为步骤 404’，

[0185] 步骤 404’：服务器向客户端发送建立连接成功的响应并通过客户端向 SDKey 发送电子书数据；

[0186] 具体为，

[0187] 步骤 404’-1：服务器将所请求下载的电子书数据用服务器备份的对称下载密钥或第一次下载时客户端传送给服务器的对称下载密钥进行加密，形成电子书的第一密文数据，并将第一密文数据通过客户端发送给 SD Key；

[0188] 步骤 404’-2：SD Key 将接收到的第一密文数据用存储的与加密相对应的对称下载密钥进行解密，生成第二明文数据，并将第二明文数据再用存储的对称阅读密钥或阅读私钥或阅读公钥再次进行加密，得到第二密文数据，并将第二密文数据保存在存储区中。

[0189] 该方法中的步骤 404 和步骤 404’还可以为：

[0190] 服务器直接通过客户端向 SD Key 发送电子书数据。

[0191] 如下为本实施例三提供的 SD Key 通过客户端下载电子书数据的第二方法，具体为：

[0192] 步骤 501：SD Key 与客户端主机建立连接；

[0193] 步骤 502：客户端向服务器发出建立连接的请求；

[0194] 优选的，SD Key 的安全区域中预置一非对称密钥，本方法称为非对称下载密钥，与其对应的服务器数据库中事先已保存有该下载公钥的备份，下载私钥则保存在 SD Key 安全区域内，不能导出 SD Key 外；或 SD Key 的安全区域中预置一非对称密钥，本方法称为非对称下载密钥，在第一次下载时，客户端将 SD Key 的下载公钥传送给服务器，服务器将下载公钥保存在数据库中，下载私钥则保存在 SD Key 安全区域内，不能导出 SD Key 外；或在第一次下载时，SD Key 产生一非对称密钥，本方法称为非对称下载密钥，客户端将 SD Key 的下载公钥传送给服务器，服务器将下载公钥保存在数据库中，下载私钥则保存在 SD Key 安全区域内，不能导出 SD Key 外；

[0195] 步骤 503：服务器通过客户端对 SD Key 进行验证并判断验证是否通过；

[0196] 具体的，

[0197] 步骤 503-1：服务器接收到客户端发送的建立连接请求以后，立即产生一随机数，将该随机数作为随机密钥通过客户端发送给 SD Key；该随机数可以采用 128 字节的二进制数。

[0198] 步骤 503-2：SD Key 接收服务器通过客户端发送的随机密钥，并使用下载私钥对该随机密钥进行签名，客户端再将签名结果作为认证数据传回给服务器；

[0199] 步骤 503-3：服务器用数据库中存储的下载公钥备份或在第一次下载时，客户端发送给服务器的下载公钥对客户端传回的认证数据进行解密验证，并判断解密之后的随机密钥是否与服务器发送给 SD Key 的随机密钥相同；

[0200] 如果是，SD Key 通过客户端与服务器建立连接成功，客户端通过网页 ActiveX 控件技术或运行在客户端的程序访问 SD Key，继续执行步骤 504；

[0201] 如果否，服务器停止操作；

[0202] 步骤 504：服务器向客户端发送建立连接成功的响应并通过客户端向 SD Key 发送

电子书数据；

[0203] 步骤 504-1：服务器将所请求下载的电子书数据用服务器数据库中备份的下载公钥或第一次下载时客户端传送给服务器的下载公钥进行加密，形成电子书的第一密文数据，并将第一密文数据通过客户端发送给 SD Key；

[0204] 步骤 504-2：SD Key 将接收到的第一密文数据保存在存储区域内；

[0205] 以上的方法是客户端下载电子书数据的下载密钥和电子书硬件访问电子书数据的阅读密钥采用同一非对称密钥；为增加对电子书数据的保护，以上下载密钥和阅读密钥可采用两对不同的非对称密钥，其中上述步骤 504 还可以替代为步骤 504'，

[0206] 步骤 504'：服务器向客户端发送建立连接成功的响应并通过客户端向 SD Key 发送电子书数据；

[0207] 具体为，

[0208] 步骤 504'-1：服务器将所请求下载的电子书数据用服务器备份的下载公钥或第一次下载时客户端传送给服务器的下载公钥进行加密，形成电子书的第一密文数据，并将第一密文数据通过客户端发送给 SD Key；

[0209] 步骤 504'-2：SD Key 将接收到的第一密文数据用存储的与加密相对应的下载私钥进行解密，生成第二明文数据，并将第二明文数据再用存储的对称阅读密钥或阅读私钥或阅读公钥再次进行加密，得到第二密文数据，并将第二密文数据保存在存储区中。

[0210] 该方法中的步骤 504 和步骤 504'还可以为：

[0211] 服务器直接通过客户端向 SD Key 发送电子书数据。

[0212] 如下为本实施例三提供的 SD Key 通过客户端下载电子书数据的第三方法，具体为：

[0213] 步骤 601：SD Key 与客户端主机建立连接；

[0214] 步骤 602：客户端向服务器发出建立连接的请求；

[0215] 优选的，SD Key 的安全区域中预置一非对称密钥，本方法称为非对称下载密钥，与其对应的服务器数据库中事先已保存有该下载公钥的备份，下载私钥则保存在SD Key安全区域内，不能导出 SD Key 外；或 SD Key 的安全区域中预置一非对称密钥，本方法称为非对称下载密钥，在第一次下载时，客户端将SD Key的下载公钥传送给服务器，服务器将下载公钥保存在数据库中，下载私钥则保存在 SD Key 安全区域内，不能导出 SD Key 外；或在第一次下载时，SD Key 产生一个非对称密钥，本方法称为非对称下载密钥，客户端将 SD Key 的下载公钥传送给服务器，服务器将下载公钥保存在数据库中，下载私钥则保存在 SD Key 安全区域内，不能导出 SD Key 外；

[0216] 步骤 603：服务器通过客户端对 SD Key 进行验证并判断验证是否通过；

[0217] 具体的，

[0218] 步骤 603-1：服务器接收到客户端发送的建立连接请求以后，立即产生一随机数，将该随机数作为随机密钥通过客户端发送给 SD Key；该随机数可以采用 128 字节的二进制数。

[0219] 步骤 603-2：SD Key 接收服务器通过客户端发送的随机密钥，并使用下载私钥对该随机密钥进行签名，客户端再将签名结果作为认证数据传回给服务器；

[0220] 步骤 603-3：服务器用数据库中存储的下载公钥备份或在第一次下载时，客户端

发送给服务器的下载公钥对SD Key传回的认证数据进行解密验证，并判断解密之后的随机密钥是否与发送给 SD Key 的随机密钥相同；

[0221] 如果是，客户端与服务器建立连接成功，客户端通过网页 ActiveX 控件技术或运行在客户端的程序访问 SD Key，继续执行步骤 604；

[0222] 如果否，服务器拒绝客户端的请求；

[0223] 步骤 604：服务器向客户端发送建立连接成功的响应并通过客户端向 SD Key 发送电子书数据；

[0224] 具体为，

[0225] 步骤 604-1：服务器产生一随机数作为对称密钥，本方法称为会话密钥；

[0226] 步骤 604-2：服务器将所请求下载的电子书数据用产生的会话密钥进行加密，形成电子书的第一密文数据；

[0227] 优选的，该随机数具体可以是一个随机数，如“书籍的备案号 + 下载时间”或“书籍的备案号 + 下载次数”；也可以是一个随机数的摘要值或散列值，如“书籍的备案号 + 下载时间”的摘要值或散列值或“书籍的备案号 + 下载次数”的摘要值或散列值，每次下载都是一密，即保证了“一次下载一密”。

[0228] 步骤 604-3：服务器将该会话密钥用服务器数据库中备份的下载公钥或第一次下载时 SD Key 传送给服务器的下载公钥进行加密，形成加密后的会话密钥；

[0229] 步骤 604-4：服务器将第一密文数据和加密后的会话密钥一起发送给 SDKey；

[0230] 步骤 604-5：SD Key 将接收到的第一密文数据和加密后的会话密钥保存在存储区域中。

[0231] 需要说明的是步骤 604-2 和步骤 604-3 可以互换顺序。

[0232] 以上的方法是客户端下载电子书数据的下载密钥和电子书硬件访问电子书数据的阅读密钥采用同一非对称密钥；为增加对电子书数据的保护，以上下载密钥和阅读密钥可采用两对不同的非对称密钥，其中上述步骤 604 还可以替代为步骤 604’，

[0233] 步骤 604’：服务器向客户端发送建立连接成功的响应并通过客户端向 SDKey 发送电子书数据；

[0234] 具体为，

[0235] 步骤 604’-1：服务器产生一随机数作为对称密钥，本方法称为会话密钥，

[0236] 步骤 604’-2：服务器将所请求下载的电子书数据用产生的会话密钥进行加密，形成电子书的第一密文数据；

[0237] 优选的，该随机数具体可以是一个随机数，如“书籍的备案号 + 下载时间”或“书籍的备案号 + 下载次数”；也可以是一个随机数的摘要值或散列值，如“书籍的备案号 + 下载时间”的摘要值或散列值或“书籍的备案号 + 下载次数”的摘要值或散列值，每次下载都是一密，即保证了“一次下载一密”。

[0238] 步骤 604’-3：服务器将该会话密钥用服务器数据库中备份的下载公钥或第一次下载时客户端传送给服务器的下载公钥进行加密，形成加密后的会话密钥；

[0239] 步骤 604’-4：服务器将第一密文数据和加密后的会话密钥通过客户端一起发送给 SD Key；

[0240] 步骤 604’-5：SD Key 将接收到的加密后的会话密钥用存储的相应地下载私钥进

行解密，得到会话密钥，并用会话密钥对接收到的第一密文数据进行解密，得到第二明文数据；

[0241] 步骤 604’-6：SD Key 将第二明文数据再用存储的对应的对称阅读密钥或阅读私钥或阅读公钥进行加密，得到第二密文数据，并将第二密文数据保存在存储区中。

[0242] 需要说明的是步骤 604’-2 和步骤 604’-3 可以互换顺序；

[0243] 该方法中的步骤 604 和步骤 604’还可以为：

[0244] 服务器直接通过客户端向 SD Key 发送电子书数据。

[0245] 本实施例所述的以上各方法中，对称下载密钥和非对称下载密钥统称为下载密钥，所述下载公钥所指的是非对称下载密钥的公钥，所述下载私钥所指的是非对称下载密钥的私钥。

[0246] 实施例 4

[0247] 本实施例 4 是实施例 1 的第 3 步中电子书硬件访问 SD Key 中电子书数据的具体方法，但不作为对本发明的限定。

[0248] 如下为本实施例 4 提供的电子书硬件访问 SD Key 中的电子书数据的第一种方法，该方法用于下载密钥和阅读密钥采用两对不同密钥的情况，具体为：

[0249] 步骤 701：电子书硬件与 SD Key 建立连接；

[0250] 步骤 702：电子书硬件向 SD Key 发送访问电子书数据的请求，SD Key 响应电子书硬件的请求并把所申请的第二密文数据发送给电子书硬件；

[0251] 步骤 703：电子书硬件将第二密文数据用存储的对称阅读密钥或阅读公钥进行解密，如果此对称阅读密钥或阅读公钥与对明文数据进行加密时的对称阅读密钥或阅读私钥相匹配，则可将第二密文数据解密得到明文数据，电子书硬件读取明文数据并输出到显示器；否则将不能正常显示明文数据。

[0252] 或，

[0253] 电子书硬件将密文数据用存储的阅读私钥进行解密，如果此阅读私钥与加密第二明文数据所使用的阅读公钥相匹配，则可将第二密文数据解密得到明文数据，电子书硬件读取明文数据并输出到显示器；否则将不能正常显示明文数据；

[0254] 如下为本实施例提供的电子书硬件访问 SD Key 中的电子书数据的第二种方法，该方法用于下载密钥和阅读密钥采用两对不同密钥的情况，具体为：

[0255] 步骤 801：电子书硬件与 SD Key 建立连接；

[0256] 步骤 802：电子书硬件向 SD Key 发送访问电子书数据的请求，SD Key 响应电子书硬件的请求后，电子书硬件读取该 SD Key 的硬件序列号或 SD Key 将自身的硬件序列号发送给电子书硬件，电子书硬件将该硬件序列号与绑定时存储的硬件序列号进行比较并判断是否一致，如果否，则电子书硬件访问 SD Key 失败。

[0257] 如果是，则执行步骤 803，

[0258] 步骤 803：电子书硬件向 SD Key 发送一个判断一致的响应，然后 SD Key 将所请求的第二密文数据发送给电子书硬件，电子书硬件取得与该硬件序列号相对应的对称阅读密钥或阅读公钥，并将第二密文数据用该阅读密钥或阅读公钥进行解密，则可得到明文数据，电子书硬件访问明文数据并输出到显示器；

[0259] 或步骤 803 替换为步骤 803’

[0260] 步骤 803’：电子书硬件向 SD Key 发送一个判断一致的响应，SD Key 用与该硬件序列号相对应的对称阅读密钥或阅读公钥或用与加密时相对应的阅读私钥对所请求的第二密文数据进行解密，得到电子书明文数据，并将明文数据发送给电子书硬件，电子书硬件访问明文数据并输出到显示器；

[0261] 如下为本实施例提供的电子书硬件访问 SD Key 中的电子书数据的第三种方法，该方法用于下载访问电子书数据采用一对密钥的情况，具体为：

[0262] 步骤 901：电子书硬件与 SD Key 建立连接；

[0263] 步骤 902：电子书硬件向 SD Key 发送访问电子书数据的请求，SD Key 响应电子书硬件的请求后，电子书硬件读取的该 SD Key 的硬件序列号或该 SD Key 将其自身的硬件序列号发送给电子书硬件，电子书硬件将该硬件序列号与绑定时存储的硬件序列号进行比较并判断是否一致，如果否，则电子书硬件访问 SD Key 失败。

[0264] 如果是，则执行步骤 903；

[0265] 步骤 903：SD Key 向电子书硬件发送一个判断一致的响应并将所请求的第一密文数据用与该硬件序列号相对应的对称阅读密钥或阅读公钥或用与加密时相对应的阅读私钥进行解密，则可将第一密文数据解密得到明文数据，电子书硬件读取明文数据并输出到显示器；

[0266] 或；

[0267] SD Key 向电子书硬件发送一个判断一致的响应并将加密后的会话密钥用与加密时对应的下载私钥进行解密，得到会话密钥，并用会话密钥对第一密文数据进行解密，得到电子书明文数据，电子书硬件读取明文数据并输出到显示器；

[0268] 如下为本实施例提供的电子书硬件访问 SD Key 中电子书数据的第四种方法，该方法用于下载访问电子书数据采用一对密钥的情况，具体为：

[0269] 电子书硬件与 SD Key 建立连接后，电子书硬件向 SD Key 发送访问电子书数据的请求，所述 SD Key 响应该请求并把第一密文数据发送给电子书硬件或不作响应直接将第一密文数据发送给电子书硬件；

[0270] 所述电子书硬件使用其保存的阅读密钥对所述第一密文数据进行解密，解密成功则所述电子书硬件的显示器上显示被访问的电子书数据；解密失败则所述显示器上显示乱码。

[0271] 实施例 5

[0272] 参见图 3，为本实施例 5 提供的第一电子书数据下载和访问的系统图，具体包括服务器 10、客户端 20、SD Key30 和电子书硬件 40，具体为：

[0273] 服务器 10 具体包括第一接收模块 11、第一存储模块 12、第一发生模块 13、第一验证模块 14、第一执行模块 15、第一发送模块 16 和第一总线模块 17；

[0274] 第一接收模块 11，用于接收第二发送模块 37 发送的对称下载密钥或下载公钥；

[0275] 第一存储模块 12，用于存储全体电子书数据和存储包含全体下载密钥或下载公钥备案的数据库；

[0276] 第一发生模块 13，用于产生随机数；

[0277] 第一验证模块 14，用于判断客户端 20 对服务器 10 发送的下载请求是否通过；

[0278] 第一执行模块 15，用于将发送给 SD Key30 的数据进行加密操作；

[0279] 第一发送模块 16，用于向 SD Key30 发送加密数据；

[0280] 第一总线模块 17，用于连接服务器 10 端的各模块，任意模块之间的通信都要经过第一总线 17 进行。

[0281] 进一步地，

[0282] 第一发生模块 13，用于产生随机数，包括，当服务器 10 通过客户端 20 对 SD Key30 进行身份验证时生成挑战码或随机密钥；

[0283] 第一发生模块 13，用于产生随机数，还包括产生会话密钥，会话密钥具体为：

[0284] 会话密钥具体可以是一个随机数，如“书籍的备案号 + 下载时间”或“书籍的备案号 + 下载次数”;会话密钥也可以是一个随机数的摘要值或散列值，如“书籍的备案号 + 下载时间”的摘要值或散列值或“书籍的备案号 + 下载次数”的摘要值或散列值。

[0285] 第一验证模块 14，用于验证与服务器 10 进行通讯的客户端 20 上插入的 SDKey30 的身份，具体为：

[0286] 当客户端 20 向服务器 10 发出下载请求时，在第一存储模块 12 的下载密钥或下载公钥备案数据库中查询所述下载请求中的 SD Key30 下载密钥或下载公钥的备案，；

[0287] 如果数据库中无该密钥的备案，服务器 10 拒绝客户端 20 的请求；

[0288] 如果数据库中有该密钥的备案，第一验证模块 14 通知第一发生模块 13 生产挑战码；

[0289] 第一验证模块 14，还用于当第一发生模块 13 产生挑战码以后，用第一存储模块 12 中的 SD Key30 对称下载密钥或下载公钥备案对挑战码进行运算，得到认证数据，验证模块 14 将认证数据与 SD Key30 传回的响应数据结果进行比较，并判断比较结果是否一致；

[0290] 如果是，服务器 10 响应客户端 20 的请求并通过客户端 20 向 SD Key30 发送电子书密文数据；

[0291] 如果否，服务器 10 拒绝客户端 20 的请求。

[0292] 第一验证模块 14，还用于对客户端 20 传回的认证数据进行解密得到随机密钥，并将随机密钥与第一发生模块 13 产生的随机密钥进行比较，并判断比较结果是否一致；

[0293] 如果是，服务器 10 响应客户端 20 的请求并通过客户端 20 向 SD Key30 发送电子书密文数据；

[0294] 如果否，服务器 10 拒绝客户端 20 的请求。

[0295] 第一执行模块 15，用于将发送给 SD Key 30 的数据进行加密，具体包括，第一执行模块 15 将所申请的电子书数据用第一存储模块 12 的数据库中的对称下载密钥或下载公钥备案进行加密处理，生成第一密文数据；

[0296] 第一执行模块 15，用于将发送给 SD Key 30 的数据进行加密，还包括，用第一发生模块 13 产生的会话密钥对所申请的电子书数据进行加密处理，形成第一密文数据，并用第一存储模块 12 的数据库中的对称下载密钥或下载公钥备案将会话密钥进行加密处理，形成加密后的会话密钥；

[0297] 第一发送模块 16，用于通过客户端 20 向 SD Key30 发送加密数据，具体包括，SD Key30 发送随机数生成模块 13 产生的挑战码或随机数。

[0298] 第一发送模块 16，还用于将所述第一密文数据通过客户端 20 发送给 Key30 或将所述第一密文数据和加密后的会话密钥通过客户端 20 一起发送给 SDKey30。

[0299] 相应地，客户端 20，用于与 SD Key30 进行连接，并用于与服务器 10 进行通信，保证了 SD Key30 和服务器 10 之间的数据交换；

[0300] 相应地，SD Key30 具体包括第二接口模块 31、第二接收模块 32、第二存储模块 33、第二执行模块 34、第二发生模块 35、第二解密模块 36、第二发送模块 37 和第二总线模块 38；

[0301] 第二接口模块 31，用于将 SD Key30 分别与客户端 20 和电子书硬件 40 的设备连接；

[0302] 优选的，SD Key30 是具有标准 SD 卡接口的信息安全装置，同时具有加密锁和存储器的功能。

[0303] 第二接收模块 32，用于接收第一发送模块 16 发送的第一加密数据并存储到第二存储模块 33 中，还用于接收第三发送模块 46 发送的对称阅读密钥或阅读公钥；；

[0304] 第二存储模块 33，用于存储电子书数据或者电子书硬件 40 传送的密钥，还用于存储事先预置的密钥或由第二发生模块 35 产生的密钥；

[0305] 第二执行模块 34，用于对数据或密钥进行加 / 解密操作；

[0306] 第二发生模块 35，用于产生对称阅读密钥或非对称阅读密钥；

[0307] 第二解密模块 36，用于将第二存储模块 33 中的密文数据解密成明文数据；

[0308] 第二发送模块 37，用于向电子书硬件 40 发送第二解密模块 36 中的明文数据或第二存储模块 33 中的密文数据，还用于将第二发生模块 35 中产生的对称阅读密钥或阅读公钥，还用于将第二发生模块 35 中的对称下载密钥或下载公钥通过客户端 20 发送给第一接收模块 11，还用于向电子书硬件 40 发送 SD Key30 的硬件序列号；

[0309] 第二总线模块 38 用于连接 SD Key30 中的各硬件模块，任意硬件模块之间的通信都要经过第二总线模块 38 进行。

[0310] 进一步地，

[0311] 第二存储模块 33，用于存储事先预置的下载密钥，还用于存储第二发生模块 35 产生的对称或非对称下载密钥；

[0312] 第二存储模块 33，用于存储事先预置的阅读密钥，还用于存储第二发生模块 35 产生的对称或非对称阅读密钥；

[0313] 第二存储模块 33，还用于存储服务器 10 下发的密文数据或存储服务器 10 下发的密文数据和加密后的会话密钥，还用于存储电子书 40 发送的对称阅读密钥或阅读公钥和由第二执行模块 35 生成的第二密文数据；

[0314] 第二执行模块 34，用于对数据进行加 / 解密操作，具体为，对服务器 10 下发的挑战码进行加密，将加密结果作为响应数据，还用于对服务器 10 发送的随机数进行加密，将加密结果作为认证数据；

[0315] 第二执行模块 34，还用于将服务器 10 下发的密文数据用第二存储模块 33 中的对称下载密钥或下载私钥进行解密，生成第二明文数据，并将第二明文数据再用第二存储模块 33 中对称阅读密钥或阅读公钥或阅读私钥进行加密，形成第二密文数据，第二执行模块 34 将第二密文数据保存在第二存储模块 33 内；

[0316] 第二执行模块 34，还用于利用第二存储模块 33 中的对称下载密钥或下载私钥对第一执行模块 15 产生的加密后的会话密钥进行解密，得到会话密钥，再用第二存储模块 33

中的会话密钥对第一密文数据进行解密，得到第二明文数据，第二执行模块 34 还用第二存储模块 33 中的对称阅读密钥或阅读公钥或阅读私钥再次对第二明文数据进行加密处理，生成第二密文数据，第二执行模块 34 将第二密文数据保存在存第二储模块 33 内。

[0317] 相应地，电子书硬件 40 具体包括第三接口模块 41、第三访问模块 42、第三存储模块 43、第三发生模块 44、第三执行模块 45、第三发送模块 46、第三接收模块 47、显示模块 48、第三总线模块 49 ；

[0318] 第三接口模块 41，用于 SD Key 30 与电子书硬件 40 的设备硬件连接 ；

[0319] 第三访问模块 42，用于向 SD Key30 发送访问电子书数据的请求，还用于绑定时读取 SD Key 30 的硬件序列号，还用于电子书硬件 40 访问 SD Key30 中电子书数据时读取 SD Key30 的硬件序列号 ；

[0320] 第三存储模块 43，用于存储 SD Key30 发送的对称阅读密钥或阅读公钥，还用于存储电子书硬件事先预置的或随机产生的对称阅读密钥或非对称阅读密钥，还用于存储第二发送模块 37 发送的 SD Key30 硬件序列号 ；

[0321] 第三发生模块 44，用于产生对称下载密钥或非对称下载密钥 ；

[0322] 第三执行模块 45，用于将 SD Key30 下发的第一密文数据或第二密文数据用第三存储模块 43 中的对称阅读密钥或阅读公钥进行解密，得到明文数据，还用于将 SD Key30 下发的第一密文数据或第二密文数据用第三存储模块 43 存储的阅读私钥进行解密，得到明文数据 ；

[0323] 第三执行模块 45，还用于将第三存储模块 43 中的 SD Key30 硬件序列号与电子书硬件 40 访问 SD Key30 中电子书数据时读取 SD Key30 的硬件序列号进行比较，并判断比较结构是否一致 ；

[0324] 第三发送模块 46，用于将第三发生模块 44 产生的对称阅读密钥或阅读公钥发送给 SD Key30 的第二接收模块 32 ；

[0325] 第三接收模块 47，用于接收第二发送模块 37 发送的明文数据或密文数据，还用于接收第二发送模块 37 发送的对称阅读密钥或阅读公钥 ；

[0326] 显示模块 48，与第三访问模块 42 相连，用于将第三执行模块 45 解密出来的明文数据或第三接收模块 47 中的明文数据显示在屏幕上 ；

[0327] 第三总线模块 49，用于连接电子书硬件 40 中的各硬件模块，任意硬件模块之间的通信都要经过第三总线模块 49 进行。

[0328] 以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

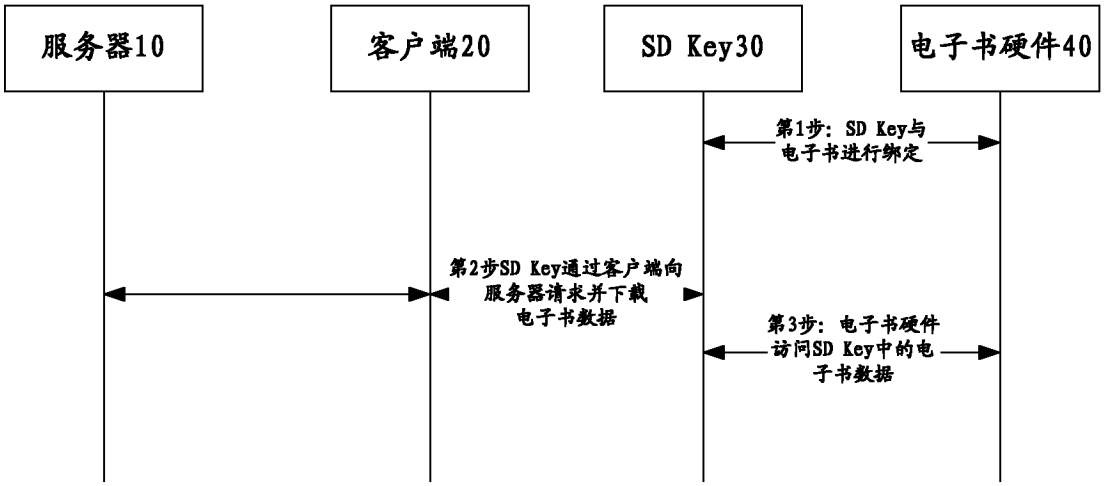

服务器10
客户端20
SD Key30
电子书硬件40
第1步：SD Key与电子书进行绑定
第2步SD Key通过客户端向服务器请求并下载电子书数据
第3步：电子书硬件访问SD Key中的电子书数据

图 1

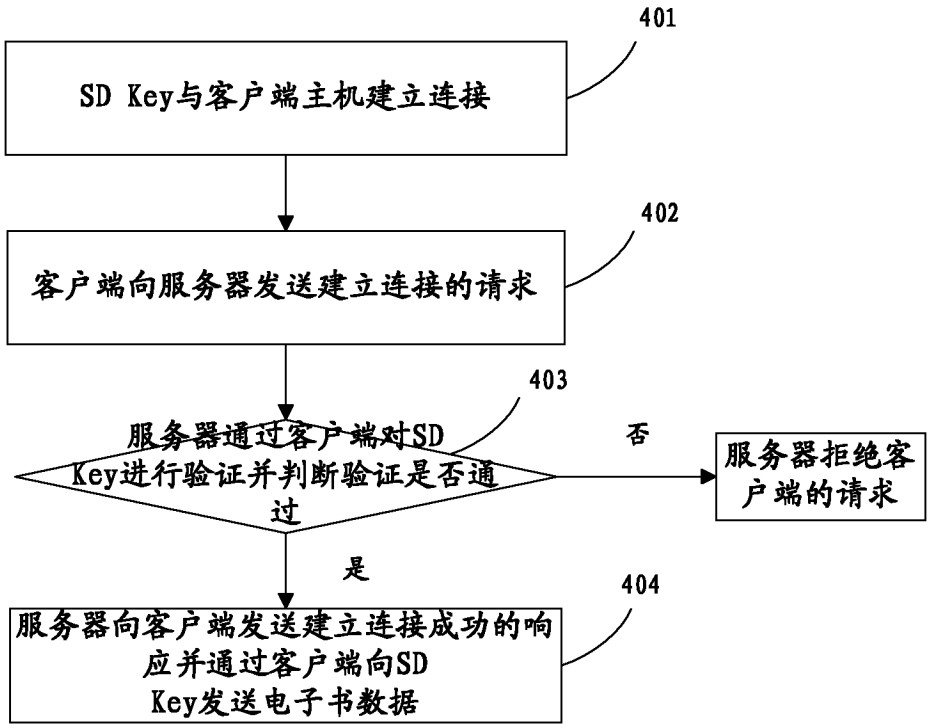

401
SD Key与客户端主机建立连接
402
客户端向服务器发送建立连接的请求
403
服务器通过客户端对SD Key进行验证并判断验证是否通过
否
服务器拒绝客户端的请求
是
404
服务器向客户端发送建立连接成功的响应并通过客户端向SD Key发送电子书数据

图 2

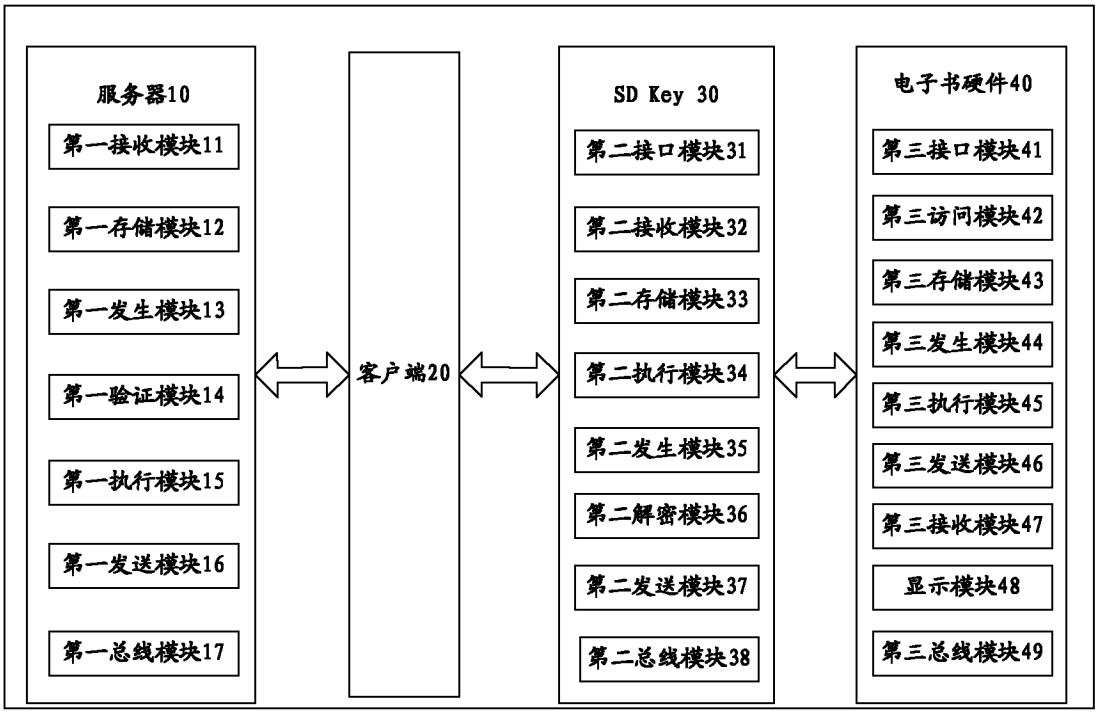

服务器10
第一接收模块11
第一存储模块12
第一发生模块13
第一验证模块14
第一执行模块15
第一发送模块16
第一总线模块17
客户端20
SD Key 30
第二接口模块31
第二接收模块32
第二存储模块33
第二执行模块34
第二发生模块35
第二解密模块36
第二发送模块37
第二总线模块38
电子书硬件40
第三接口模块41
第三访问模块42
第三存储模块43
第三发生模块44
第三执行模块45
第三发送模块46
第三接收模块47
显示模块48
第三总线模块49

图 3