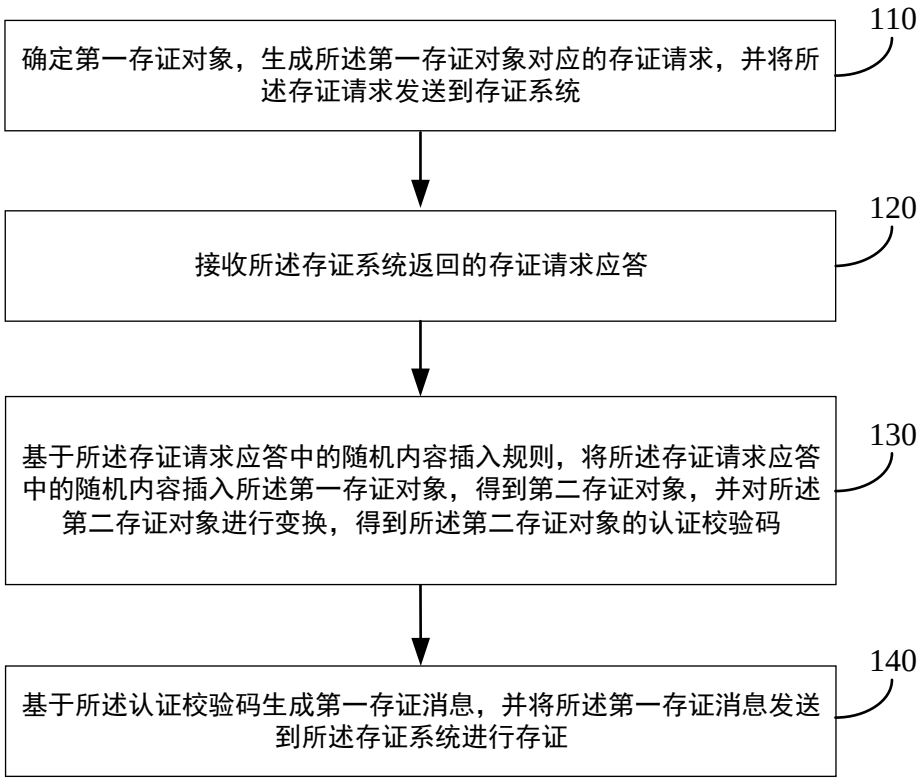
说　明　书　摘　要

本发明提供一种低开销抗泄漏与伪造的存证方法、装置、设备和存储介质，其中方法包括：确定第一存证对象，生成第一存证对象对应的存证请求，并将存证请求发送到存证系统；接收存证系统返回的存证请求应答；基于存证请求应答中的随机内容插入规则，将存证请求应答中的随机内容插入第一存证对象，得到第二存证对象，并对第二存证对象进行变换，得到第二存证对象的认证校验码；基于认证校验码生成第一存证消息，并将第一存证消息发送到存证系统进行存证。本发明基于认证校验码生成的存证消息不包括存证对象内容且受存证系统约束，因此存证对象内容不被泄露、不能伪造，降低了传输与存储存证对象内容的开销，并提高存证的可信度和证据检索效率。

摘　要　附　图


110
确定第一存证对象，生成所述第一存证对象对应的存证请求，并将所述存证请求发送到存证系统
120
接收所述存证系统返回的存证请求应答
130
基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，并对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码
140
基于所述认证校验码生成第一存证消息，并将所述第一存证消息发送到所述存证系统进行存证

权　利　要　求　书

1、一种低开销抗泄漏与伪造的存证方法，其特征在于，应用于信息系统，所述存证方法包括：

确定第一存证对象，生成所述第一存证对象对应的存证请求，并将所述存证请求发送到存证系统；

接收所述存证系统返回的存证请求应答；

基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，并对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码；

基于所述第二存证对象的认证校验码生成第一存证消息，并将所述第一存证消息发送到所述存证系统进行存证。

2、根据权利要求 1 所述的低开销抗泄漏与伪造的存证方法，其特征在于，所述生成所述第一存证对象对应的存证请求，包括：

基于所述第一存证对象的类型，生成所述第一存证对象对应的存证请求；

或者，

基于所述第一存证对象的类型，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统标识、信息系统的网络地址、信息系统的硬件地址、信息系统的业务内部索引号、第一存证对象的大小、第一存证对象内容的描述和待生成的存证请求内容完整性的度量值及签名中的至少一种，生成所述第一存证对象对应的存证请求。

3、根据权利要求 1 所述的低开销抗泄漏与伪造的存证方法，其特征在于，所述基于所述第二存证对象的认证校验码生成第一存证消息，包括：

基于信息系统标识和第二存证对象的认证校验码，生成第一存证消息；

或者，

基于信息系统标识和第二存证对象的认证校验码，以及所述第一存证对象的操作主体、第一存证对象的操作行为、协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统的网络地址、信息系统的硬件地址、存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、密文字段和待生成的第一存证消息完整性的度量值及签名中的至少一种，生成第一存证消息。

4、根据权利要求 1 至 3 中任一项所述的低开销抗泄漏与伪造的存证方法，其特征在于，所述存证系统包括中心存证系统和本地存证系统；

所述将所述存证请求发送到存证系统，包括：

将所述存证请求直接发送至所述中心存证系统，或者，将所述存证请求发送至所述本地存证系统，以使所述本地存证系统将所述存证请求发送至所述中心存证系统；

所述接收所述存证系统返回的存证请求应答，包括：

接收所述中心存证系统直接返回的存证请求应答，或者，接收所述中心存证系统返回并经过所述本地存证系统发送的存证请求应答。

5、根据权利要求 1 至 3 中任一项所述的低开销抗泄漏与伪造的存证方法，其特征在于，所述存证系统包括中心存证系统和本地存证系统；

所述将所述第一存证消息发送到所述存证系统进行存证，包括：

将所述第一存证消息直接发送所述中心存证系统，以使所述中心

存证系统基于所述第一存证消息向所述信息系统返回第二存证收条；

接收所述第二存证收条；

或者，

将所述第一存证消息发送到所述本地存证系统，以使所述本地存证系统基于所述第一存证消息生成第二存证消息，并由所述本地存证系统将所述第二存证消息发送至所述中心存证系统，所述中心存证系统基于所述第二存证消息向所述本地存证系统返回第二存证收条；

接收所述本地存证系统基于所述第二存证收条返回的第一存证收条。

6、一种低开销抗泄漏与伪造的存证方法，其特征在于，应用于存证系统，所述低开销抗泄漏与伪造的存证方法包括：

接收信息系统发送的存证请求，所述存证请求与第一存证对象对应；

获取与所述存证请求对应的存证请求应答；

将所述存证请求应答返回到所述信息系统，以使所述信息系统基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码，并基于所述第二存证对象的认证校验码生成第一存证消息；

基于所述信息系统发送的第一存证消息进行存证。

7、根据权利要求 6 所述的低开销抗泄漏与伪造的存证方法，其特征在于，所述获取与所述存证请求对应的存证请求应答，包括：

基于所述存证请求中所述第一存证对象的类型，确定所述随机内容插入规则；

或者，

基于所述存证请求中所述第一存证对象的类型，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定

义字段、信息系统标识、信息系统的网络地址、信息系统的硬件地址、信息系统的业务内部索引号、第一存证对象的大小、第一存证对象内容的描述和存证请求内容完整性的度量值及签名中的至少一种，确定所述随机内容插入规则；

生成所述随机内容；

基于所述随机内容插入规则和所述随机内容，生成与所述存证请求对应的存证请求应答。

8、根据权利要求 7 所述的低开销抗泄漏与伪造的存证方法，其特征在于，所述基于所述随机内容插入规则和所述随机内容，生成与所述存证请求对应的存证请求应答，包括：

基于所述随机内容插入规则和所述随机内容，生成与所述存证请求对应的存证请求应答；

或者，

基于所述随机内容插入规则和所述随机内容，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、存证系统标识、存证系统的业务内部索引号、信息系统的业务内部索引号、请求应答时间、密文字段和待生成的存证请求应答内容完整性的度量值及签名中的至少一种，生成与所述存证请求对应的存证请求应答。

9、根据权利要求 6 所述的低开销抗泄漏与伪造的存证方法，其特征在于，所述存证系统包括中心存证系统和本地存证系统，在所述存证方法应用于所述中心存证系统的情况下，所述基于所述信息系统发送的存证消息进行存证，包括：

接收所述信息系统直接发送的第一存证消息，生成第二存证收条并直接返回至所述信息系统；

或者，

接收所述本地存证系统发送的第二存证消息，生成第二存证收条

返回至所述本地存证系统，以使所述本地存证系统在接收到所述第二存证收条后生成第一存证收条，并将所述第一存证收条返回至所述信息系统，或者通过所述本地存证系统所述第二存证收条发送至所述信息系统，所述第二存证消息是所述本地存证系统基于所述第一存证消息生成的。

10、根据权利要求 9 所述的低开销抗泄漏与伪造的存证方法，其特征在于，所述生成第二存证收条并直接返回至所述信息系统，包括：基于中心存证系统标识，生成第二存证收条并直接返回至所述信息系统；

或者，

基于中心存证系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、信息系统标识、信息系统的网络地址、信息系统的硬件地址、中心存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的类型、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、密文字段、第一存证消息完整性的度量值及签名和待生成的第二存证收条完整性的度量值及签名中的至少一种，生成第二存证收条并直接返回至所述信息系统。

11、根据权利要求 9 所述的低开销抗泄漏与伪造的存证方法，其特征在于，所述生成第二存证收条返回至所述本地存证系统，包括：

基于中心存证系统标识，生成第二存证收条返回至所述本地存证系统；

或者，

基于中心存证系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、信息系统标识、中心存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第二存证对象的认证校验码、第一存证消息完整性的度量值及签名、第二存证消息完整性的度量值及签名和待生成的第二存证收条完整性的度量值及签名中的至少一种，生成第二存证收条返回至所述本地存证系统；

12、根据权利要求 6 所述的低开销抗泄漏与伪造的存证方法，其特征在于，所述存证系统包括中心存证系统和本地存证系统，在所述存证方法应用于所述本地存证系统的情况下，所述基于所述信息系统发送的存证消息进行存证，包括：

接收所述第一存证消息，并基于信息系统标识生成第二存证消息；

或者，

接收所述第一存证消息，并基于信息系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统的网络地址、信息系统的硬件地址、本地存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、第一存证消息完整性的度量值及签名和待生成的第二存证消息完整性的度量值及签名中的至少一种，生

成第二存证消息；

将所述第二存证消息发送至所述中心存证系统，以使所述中心存证系统在接收到所述第二存证消息后生成第二存证收条；

在接收到所述中心存证系统返回的第二存证收条后，生成第一存证收条返回所述信息系统。

13、根据权利要求 12 所述的低开销抗泄漏与伪造的存证方法，其特征在于，所述生成第一存证收条返回所述信息系统，包括：

基于本地存证系统标识，生成第一存证收条返回所述信息系统；

或者，

基于本地存证系统标识，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、第一存证收条标识、第一存证收条时间、信息系统标识、信息系统的网络地址、信息系统的硬件地址、中心存证系统的业务内部索引号、本地存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、密文字段、第一存证消息完整性的度量值及签名、第二存证消息完整性的度量值及签名、第二存证收条完整性的度量值及签名和待生成的第一存证收条完整性的度量值及签名中的至少一种，生成第一存证收条返回所述信息系统。

14、一种低开销抗泄漏与伪造的存证装置，其特征在于，应用于信息系统，所述低开销抗泄漏与伪造的存证装置包括：

请求发送单元，用于确定第一存证对象，生成所述第一存证对象

对应的存证请求，并将所述存证请求发送到存证系统；

应答接收单元，用于接收所述存证系统返回的存证请求应答；

认证校验码生成单元，用于基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，并对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码；

存证发送单元，用于基于所述认证校验码生成第一存证消息，并将所述第一存证消息发送到所述存证系统进行存证。

15、一种低开销抗泄漏与伪造的存证装置，其特征在于，应用于存证系统，所述低开销抗泄漏与伪造的存证装置包括：

请求接收单元，用于接收信息系统发送的存证请求，所述存证请求与第一存证对象对应；

应答获取单元，用于获取与所述存证请求对应的存证请求应答；

应答返回单元，用于将所述存证请求应答返回到所述信息系统，以使所述信息系统基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码，并基于所述认证校验码生成第一存证消息；

存证单元，用于基于所述信息系统发送的第一存证消息进行存证。

16、一种电子设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如权利要求 1 至 13 任一项所述低开销抗泄漏与伪造的存证方法。

17、一种非暂态计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求 1 至 13 任一项所述低开销抗泄漏与伪造的存证方法。

{case_no}

说　明　书

低开销抗泄漏与伪造的存证方法、装置、设备和存储介质

技术领域

本发明涉及大数据技术领域，尤其涉及一种低开销抗泄漏与伪造的存证方法、装置、设备和存储介质。

背景技术

当个人信息在网络和系统间流转和使用的过程中，为了确保系统内部或跨系统监管的证据可靠，通常需要对操作情况进行存证和审计，且需要采取一定的技术手段来防止审计日志或被存证对象内容被伪造，即审计日志或被存证对象内容在事件发生后被篡改或伪造。

传统审计日志方法，是通过单位内部的信息系统审计日志实现监管，这种监管方式的审计日志用于内部监管。但对于执法监管部门而言，审计日志和被存证对象内容均存放在被监管的信息系统内，审计日志和被存证对象内容都存在被伪造的可能，致使以审计日志作为监管的证据对执法监管部门是不完全可信的。

为了防止审计日志和被存证对象内容被伪造，可以将被存证对象内容发送给外部的第三方存证机构，由第三方存证机构对被存证对象内容进行审计存证，这种方式产生的审计存证对执法监管部门来说是可信的，但仍然难以解决共谋篡改或共谋伪造，并且因为被存证对象内容存于第三方存证机构，存在被存证对象内容的泄露风险。

综上，本专利提出一种执法监管部门和被监管的信息系统两方共同参与的低开销抗泄露与伪造的存证方法，在不需要被存证对象内容的情况下达到可信存证监管的目的。被监管的信息系统按照执法监管

部门提供的随机内容和随机内容插入规则对被存证对象内容进行变换得到被存证对象内容和随机内容融合后的认证校验码，被监管的信息系统根据此认证校验码生成存证消息，存证消息的上报过程采用加密的方式，保障了存证过程的传输安全；执法监管部门仅存储此存证消息，由于存证消息不包括被存证对象内容且受存证系统约束，因此被存证对象内容不被泄露、不能伪造，解决了审计日志或被存证对象内容在事件发生后被篡改或伪造的问题，降低了传输与被存证对象内容的开销，并提高存证的可信度和证据检索效率。此方法不仅可以用于执法监管、也可以用于企业内部自监管以及第三方测评等场景。

发明内容

本发明提供一种低开销抗泄漏与伪造的存证方法、装置、设备和存储介质，用以解决现有技术中存证信息的可信度难以保证、存在信息泄露的缺陷。

本发明提供一种低开销抗泄漏与伪造的存证方法，应用于信息系统，所述低开销抗泄漏与伪造的存证方法包括：

确定第一存证对象，生成所述第一存证对象对应的存证请求，并将所述存证请求发送到存证系统；

接收所述存证系统返回的存证请求应答；

基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，并对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码；

基于所述认证校验码生成第一存证消息，并将所述第一存证消息发送到所述存证系统进行存证。

根据本发明提供的低开销抗泄漏与伪造的存证方法，所述生成所述第一存证对象对应的存证请求，包括：

基于所述第一存证对象的类型，生成所述第一存证对象对应的存证请求；

或者，

基于所述第一存证对象的类型，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统标识、信息系统的网络地址、信息系统的硬件地址、信息系统的业务内部索引号、第一存证对象的大小、第一存证对象内容的描述和待生成的存证请求内容完整性的度量值及签名中的至少一种，生成所述第一存证对象对应的存证请求。

根据本发明提供的低开销抗泄漏与伪造的存证方法，所述基于所述第二存证对象的认证校验码生成第一存证消息，包括：

基于信息系统标识和第二存证对象的认证校验码，生成第一存证消息；

或者，

基于信息系统标识和第二存证对象的认证校验码，以及所述第一存证对象的操作主体、第一存证对象的操作行为、协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统的网络地址、信息系统的硬件地址、存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、密文字段和待生成的第一存证消息完整性的度量值及签名中的至少一种，生成第一存证消息。

根据本发明提供的低开销抗泄漏与伪造的存证方法，所述存证系统包括中心存证系统和本地存证系统；

所述将所述存证请求发送到存证系统，包括：

将所述存证请求直接发送至所述中心存证系统，或者，将所述存

证请求发送至所述本地存证系统，以使所述本地存证系统将所述存证请求发送至所述中心存证系统；

所述接收所述存证系统返回的存证请求应答，包括：

接收所述中心存证系统直接返回的存证请求应答，或者，接收所述中心存证系统返回并经过所述本地存证系统发送的存证请求应答。

根据本发明提供的低开销抗泄漏与伪造的存证方法，所述存证系统包括中心存证系统和本地存证系统；

所述将所述第一存证消息发送到所述存证系统进行存证，包括：

将所述第一存证消息直接发送所述中心存证系统，以使所述中心存证系统基于所述第一存证消息向所述信息系统返回第二存证收条；

接收所述第二存证收条；

或者，

将所述第一存证消息发送到所述本地存证系统，以使所述本地存证系统基于所述第一存证消息生成第二存证消息，并由所述本地存证系统将所述第二存证消息发送至所述中心存证系统，所述中心存证系统基于所述第二存证消息向所述本地存证系统返回第二存证收条；

接收所述本地存证系统基于所述第二存证收条返回的第一存证收条。

本发明还提供一种低开销抗泄漏与伪造的存证方法，应用于存证系统，所述低开销抗泄漏与伪造的存证方法包括：

接收信息系统发送的存证请求，所述存证请求与第一存证对象对应；

获取与所述存证请求对应的存证请求应答；

将所述存证请求应答返回到所述信息系统，以使所述信息系统基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码，并基于所

述认证校验码生成第一存证消息；

基于所述信息系统发送的第一存证消息进行存证。

根据本发明提供的一种低开销抗泄漏与伪造的存证方法，所述获取与所述存证请求对应的存证请求应答，包括：

基于所述存证请求中所述第一存证对象的类型，确定所述随机内容插入规则；

或者，

基于所述存证请求中所述第一存证对象的类型，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统标识、信息系统的网络地址、信息系统的硬件地址、信息系统的业务内部索引号、第一存证对象的大小、第一存证对象内容的描述和存证请求内容完整性的度量值及签名中的至少一种，确定所述随机内容插入规则；

生成所述随机内容；

基于所述随机内容插入规则和所述随机内容，生成与所述存证请求对应的存证请求应答。

根据本发明提供的一种低开销抗泄漏与伪造的存证方法，所述基于所述随机内容插入规则和所述随机内容，生成与所述存证请求对应的存证请求应答，包括：

基于所述随机内容插入规则和所述随机内容，生成与所述存证请求对应的存证请求应答；

或者，

基于所述随机内容插入规则和所述随机内容，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、存证系统标识、存证系统的业务内部索引号、信息系统的业务内部索引号、请求应答时间、密文字段和待生成的存证请求应答内容完整性的度量值及签名中的至少一种，生成与所述存证请求对应的存

证请求应答。

根据本发明提供的一种低开销抗泄漏与伪造的存证方法，所述存证系统包括中心存证系统和本地存证系统，在所述存证方法应用于所述中心存证系统的情况下，所述基于所述信息系统发送的存证消息进行存证，包括：

接收所述信息系统直接发送的第一存证消息，生成第二存证收条并直接返回至所述信息系统；

或者，

接收所述本地存证系统发送的第二存证消息，生成第二存证收条返回至所述本地存证系统，以使所述本地存证系统在接收到所述第二存证收条后生成第一存证收条，并将所述第一存证收条返回至所述信息系统，或者通过所述本地存证系统所述第二存证收条发送至所述信息系统，所述第二存证消息是所述本地存证系统基于所述第一存证消息生成的。

根据本发明提供的一种低开销抗泄漏与伪造的存证方法，所述生成第二存证收条并直接返回至所述信息系统，包括：

基于中心存证系统标识，生成第二存证收条并直接返回至所述信息系统；

或者，

基于中心存证系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、信息系统标识、信息系统的网络地址、信息系统的硬件地址、中心存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的类型、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、

第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、密文字段、第一存证消息完整性的度量值及签名和待生成的第二存证收条完整性的度量值及签名中的至少一种，生成第二存证收条并直接返回至所述信息系统。

根据本发明提供的一种低开销抗泄漏与伪造的存证方法，所述生成第二存证收条返回至所述本地存证系统，包括：

基于中心存证系统标识，生成第二存证收条返回至所述本地存证系统；或者，

基于中心存证系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、信息系统标识、中心存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第二存证对象的认证校验码、第一存证消息完整性的度量值及签名、第二存证消息完整性的度量值及签名和待生成的第二存证收条完整性的度量值及签名中的至少一种，生成第二存证收条返回至所述本地存证系统；

根据本发明提供的一种低开销抗泄漏与伪造的存证方法，所述存证系统包括中心存证系统和本地存证系统，在所述存证方法应用于所述本地存证系统的情况下，所述基于所述信息系统发送的存证消息进行存证，包括：

接收所述第一存证消息，并基于信息系统标识生成第二存证消息；或者，

接收所述第一存证消息，并基于信息系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统的网络地址、信息系统的硬件地址、本地存证系统的业务内

部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、第一存证消息完整性的度量值及签名和待生成的第二存证消息完整性的度量值及签名中的至少一种，生成第二存证消息；

将所述第二存证消息发送至所述中心存证系统，以使所述中心存证系统在接收到所述第二存证消息后生成第二存证收条；

在接收到所述中心存证系统返回的第二存证收条后，生成第一存证收条返回所述信息系统。

根据本发明提供的一种低开销抗泄漏与伪造的存证方法，所述生成第一存证收条返回所述信息系统，包括：

基于本地存证系统标识，生成第一存证收条返回所述信息系统；

或者，

基于本地存证系统标识，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、第一存证收条标识、第一存证收条时间、信息系统标识、信息系统的网络地址、信息系统的硬件地址、中心存证系统的业务内部索引号、本地存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、

第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、密文字段、第一存证消息完整性的度量值及签名、第二存证消息完整性的度量值及签名、第二存证收条完整性的度量值及签名和待生成的第一存证收条完整性的度量值及签名中的至少一种，生成第一存证收条返回所述信息系统。本发明还提供一种低开销抗泄漏与伪造的存证装置，应用于信息系统，所述低开销抗泄漏与伪造的存证装置包括：

请求发送单元，用于确定第一存证对象，生成所述第一存证对象对应的存证请求，并将所述存证请求发送到存证系统；

应答接收单元，用于接收所述存证系统返回的存证请求应答；

认证校验码生成单元，用于基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，并对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码；

存证发送单元，用于基于所述认证校验码生成第一存证消息，并将所述第一存证消息发送到所述存证系统进行存证。

本发明还提供一种低开销抗泄漏与伪造的存证装置，应用于存证系统，所述低开销抗泄漏与伪造的存证装置包括：

请求接收单元，用于接收信息系统发送的存证请求，所述存证请求与第一存证对象对应；

应答获取单元，用于获取与所述存证请求对应的存证请求应答；

应答返回单元，用于将所述存证请求应答返回到所述信息系统，以使所述信息系统基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码，并基于所述认证校验码生成第一存证消息；

存证单元，用于基于所述信息系统发送的第一存证消息进行存证。

本发明还提供一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现如上述任一种所述低开销抗泄漏与伪造的存证方法。

本发明还提供一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现如上述任一种所述低开销抗泄漏与伪造的存证方法。

本发明还提供一种计算机程序产品，包括计算机程序，所述计算机程序被处理器执行时实现如上述任一种所述低开销抗泄漏与伪造的存证方法。

本发明提供的低开销抗泄漏与伪造的存证方法、装置、设备和存储介质，基于第一存证对象的类型生成随机内容和随机内容插入规则，将随机内容按照随机内容插入规则插入到第一存证对象生成第二存证对象、再对第二存证对象进行变换获取第二存证对象的认证校验码，由于随机内容插入规则和随机内容是存证系统根据对象的类型进行生成、且不可变更，认证校验码具有机密性、完整性和数据源认证的特性，因此通过伪造生成具有相同语义且相同类型的存证对象理论上不可能，可以有效避免有意伪造存证对象的情况发生。存证系统存储基于第二存证对象的认证校验码生成的存证消息（仅包含认证校验码和相关管理信息），不存储存证对象的内容，既保护了存证对象的内容，消除了数据泄露的风险，还大幅度降低了数据传输带宽和存证系统的存储开销。存证消息中的业务内部索引号提升了在溯源取证过程中索引存证对象的效率。存证信息上报采用加密方式传输，保障了存证信息传输过程中的安全。本专利在抗数据伪造与泄露、降低传输带宽和存储开销、提高存储效率和证据检索效率等方面具有显著的优势，提高了存证的可信度与效率。

附图说明

为了更清楚地说明本发明或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本发明提供的存证方法的流程示意图之一；

图 2 是本发明提供的存证方法的流程示意图之二；

图 3 是本发明提供的存证方法的流程示意图之三；

图 4 是本发明提供的存证方法的流程示意图之四；

图 5 是本发明提供的存证方法的流程示意图之五；

图 6 是本发明提供的存证装置的结构示意图之一；

图 7 是本发明提供的存证装置的结构示意图之二；

图 8 是本发明提供的设备的结构示意图。

具体实施方式

为使本发明的目的、技术方案和优点更加清楚，下面将结合本发明中的附图，对本发明中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

数据抗伪造方案是为了保证存证信息可信度的手段。在数据抗伪造方案中，常见的抗伪造方案是采用数据加解密技术，该技术需要双方都拥有原始数据或加密后的原始数据。然而，当数据量较大时，硬件资源消耗会相应增加。

在某些情况下，接收方只需要验证数据的真实性而不需要获取原始数据。对于这种情况，一种更简洁的方法是使用哈希函数来判断数

据是否被篡改。

但在实际应用中，存在可以生成与原始数据一致的哈希值的伪造数据，用此类伪造数据来替换原始数据，会导致基于哈希函数的抗伪造方案失效，存证信息的可信度无法保证。

针对上述问题，本发明提供一种存证方法。图 1 是本发明提供的存证方法的流程示意图之一，如图 1 所示，该方法应用于信息系统，该方法包括：

步骤 110，确定第一存证对象，生成所述第一存证对象对应的存证请求，并将所述存证请求发送到存证系统。

此处，信息系统即证据发送方，也就是需要进行信息存证的一方。第一存证对象即由信息系统触发生成的、待存证的信息。相应地，存证系统即信息存证方，也就是用于实现信息存证的一方。

信息系统的存证触发方式包括但不限于：可以通过按钮、圈出、勾选、标记、按键、滑轮、菜单、语音、视频、眼神、手势、文字、生物电信号、虚拟环境等形式中的一种或者多种方式。具体类似手机的静音键的上下拨动、录音笔的左右拨动，也可以反映为脱离物理开关的输入，例如屏幕手势（左到右、右到左、上到下、下到上等）、弹出界面填写（例如表单录入）、文件（例如 XML 格式）导入、语音录入、配置文件输入、弹框/菜单选择、在屏幕上显示虚拟键盘输入等方式的触发。

信息系统在确定第一存证对象之后，即可对应生成存证请求，并将存证请求发送到存证系统。可以理解的是，第一存证对象与存证请求一一对应，存证请求中携带了第一存证对象的相关信息，例如第一存证对象的类型、大小、内容的描述等，存证对象的类型包括但不限于 xml、html、网页表单、图数据库节点及属性、关系型数据库表、分布式文件系统类型、txt 文本文档、版式文档（ofd、pdf 等格式）、流式文档（doc、docx、xls、xlsx、ppt、pptx 等格式）、图像（jpg、png、

psd、bmp 等格式）、音频（mp3、aac、ogg 等格式）、视频（mp4、avi、flv、wmv、mov 等格式）等，本发明实施例对此不作具体限定。

步骤 120，接收所述存证系统返回的存证请求应答。

步骤 130，基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，并对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码。

具体地，存证系统可以接收信息系统发送的存证请求，并针对存证请求返回存证请求应答。此处，存证请求应答中携带有随机内容插入规则和随机内容。随机内容是根据存证对象的类型，通过一定规则生成不同类型的内容，随机内容包括但不限于：字符串、数字、文本、图数据库的节点、关系型数据库表中的列、图像、音频、视频等。例如：存证对象是 txt 文本文档，生成的随机内容可以是不限长度的字符串、数字、文本；存证对象是关系型数据库表，生成的随机内容可以是关系型数据库表的列等。本专利对随机内容的生成规则不作具体约束，包括但不限于随机数、模运算等；本专利对随机内容、第一存证对象内容、生成的第二存证对象内容的大小等不作具体约束。

随机内容插入规则根据存证对象的类型，包括但不限于存证对象的头部、尾部，或者存证对象大小字节范围的任意字节处插入或替换等。

随机内容和随机内容插入规则的生成可以配置，配置方法可以通过按钮、圈出、勾选、标记、按键、滑轮、菜单、语音、视频、眼神、手势、文字、生物电信号、虚拟环境等形式中的一种或者多种方式。具体类似手机的静音键的上下拨动、录音笔的左右拨动，也可以反映为脱离物理开关的输入，例如屏幕手势（左到右、右到左、上到下、下到上等）、弹出界面填写（例如表单录入）、文件（例如 XML 格式）导入、语音录入、配置文件输入、弹框/菜单选择、在屏幕上显示虚拟

键盘输入等方式。

随机内容和随机内容插入规则在中心存证系统留存，用于侵权事件发生后中心存证系统的溯源取证。

信息系统在接收到存证请求应答之后，即可从中获取到随机内容插入规则和随机内容，并基于此两者，生成对第一存证对象进行存证所需的认证校验码。

在此过程中，信息系统需要基于存证请求应答中的随机内容插入规则，将存证请求应答中的随机内容插入到第一存证对象中，由此得到第二存证对象。可以理解的是，此处的第二存证对象即在第一存证对象中、在随机内容插入规则所指示的位置处插入了随机对象之后的存证对象。

在得到第二存证对象之后，即可针对第二存证对象进行变换，并将变换所得的结果，作为第二存证对象的认证校验码。此处的变换，能够实现单向不可逆的变换即可，包括但不限于：散列、SM4-GCM 等，本专利对认证校验码生成方式不作具体约束。例如：认证校验码可以采用 SM4-GCM 模式生成，SM4-GCM 是国家分组密码算法标准 SM4 算法与伽罗华/计数器模式 GCM（Galois/Counter Mode）的结合，其包含 SM4 计数器（SM4-CTR, SM4 based Counter）模式和伽罗华 Hash（GHASH, Galois Hash）模式，同时具备机密性、完整性和数据源认证特性，SM4-CTR 模式通过密钥进行加密保证了机密性和数据源认证特性，GHASH 保证了消息完整性。

可以理解的是，相较于直接针对第一存证对象进行变换所得的完整性度量值，本发明实施例中基于随机内容插入规则、将随机内容插入第一存证对象后再进行变换得到的认证校验码，通过伪造生成具有相同语义且相同类型的存证对象理论上不可能，可以有效避免有意伪造存证对象的情况发生。

步骤 140，基于所述认证校验码生成第一存证消息，并将所述第一存证消息发送到所述存证系统进行存证。

具体地，信息系统在得到第二存证对象的认证校验码之后，即可生成携带该认证校验码的第一存证消息，并将该第一存证消息发送到存证系统进行存证。

本发明实施例提供的方法，基于第一存证对象的类型生成随机内容和随机内容插入规则，将随机内容按照随机内容插入规则插入到第一存证对象生成第二存证对象、再对第二存证对象进行变换获取第二存证对象的认证校验码，由于随机内容插入规则和随机内容是存证系统根据对象的类型进行生成、且不可变更，认证校验码具有机密性、完整性和数据源认证的特性，因此通过伪造生成具有相同语义且相同类型的存证对象理论上不可能，可以有效避免有意伪造存证对象的情况发生。存证系统存储基于第二存证对象的认证校验码生成的存证消息（仅包含认证校验码和相关管理信息），不存储存证对象的内容，既保护了存证对象的内容，消除了数据泄露的风险，还大幅度降低了数据传输带宽和存证系统的存储开销。存证消息中的业务内部索引号提升了在溯源取证过程中索引存证对象的效率。存证信息上报采用加密方式传输，保障了存证信息传输过程中的安全。本专利在抗数据伪造与泄露、降低传输带宽和存储开销、提高存储效率和证据检索效率等方面具有显著的优势，提高了存证的可信度与效率。

并且，本发明实施例提供的方法，可应用于常见的标准传输协议，包括但不限于 TCP、UDP、HTTP/HTTPS 协议，以及自定义安全协议等；应用范围包括但不限于审计日志、操作证据、流转状态等内容的存证场景。

基于上述实施例，在步骤 110 中，所述生成所述第一存证对象对应的存证请求，包括：

基于所述第一存证对象的类型，生成所述第一存证对象对应的存

证请求；

或者，

基于所述第一存证对象的类型，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统标识、信息系统的网络地址、信息系统的硬件地址、信息系统的业务内部索引号、第一存证对象的大小、第一存证对象内容的描述和待生成的存证请求内容完整性的度量值及签名中的至少一种，生成所述第一存证对象对应的存证请求。

具体地，可以基于第一存证对象的类型，生成第一存证对象对应的存证请求。即，存证请求中，可以包括第一存证对象的类型，为便于说明，以下将存证请求记为 D_1。

其中，存证请求 D_1 中至少包含一种第一存证对象的类型，存证对象的类型包括但不限于 xml、html、网页表单、图数据库节点及属性、关系型数据库表、分布式文件系统类型、txt 文本文档、版式文档（ofd、pdf 等格式）、流式文档（doc、docx、xls、xlsx、ppt、pptx 等格式）、图像（jpg、png、psd、bmp 等格式）、音频（mp3、aac、ogg 等格式）、视频（mp4、avi、flv、wmv、mov 等格式）等，本发明实施例对此不作具体限定；

除此以外，还可以基于第一存证对象的类型，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统标识、信息系统的网络地址、信息系统的硬件地址、信息系统的业务内部索引号、第一存证对象的大小、第一存证对象内容的描述和待生成的存证请求内容完整性的度量值及签名中的至少一种，生成第一存证对象对应的存证请求。

即，存证请求中，除了可以包括第一存证对象的类型，还可以包括协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统标识、信息系统的网络地址、信息系统的

硬件地址、信息系统的业务内部索引号、第一存证对象的大小、第一存证对象内容的描述和待生成的存证请求内容完整性的度量值及签名中的至少一种。为便于说明，以下将存证请求记为 D_1。

将所述第一存证对象的类型，记为待生成的存证请求内容；

或者，

将所述第一存证对象的类型，以及所述信息系统标识、信息系统的网络地址、信息系统的硬件地址、信息系统的业务内部索引号、第一存证对象的大小和第一存证对象内容的描述中的至少一种，记为待生成的存证请求内容。

协议版本号是表示通信协议的版本；

命令类别用于表示信息系统与存证系统交互的类型，命令类别包括但不限于：存证请求命令、存证请求应答命令、第一存证消息上报命令、第二存证消息上报命令、第一存证收条反馈命令和第二存证收条反馈命令；

存证事项类别用于表示信息系统具体上报信息的事项种类，包括但不限于：采集、分类分级、脱敏、使用、流转、存储、删除、合规检查和评测；

消息格式版本用于表示信息系统与存证系统、存证系统间交互信息的格式，包括但不限于存证请求、请求应答、第一存证消息、第二存证消息、第一存证收条、第二存证收条、异常操作消息或其他版本的消息格式；

数据包长度是表示整个数据包的长度；

信息系统标识，包括但不限于编号，用于区分不同的信息系统；

信息系统的网络地址即 IP 地址，用于记录不同的信息系统进行业务交互的网络地址信息；

信息系统的硬件地址即 MAC 地址，用于记录不同的信息系统进行业务交互设备的信息系统的硬件地址；

信息系统的业务内部索引号是信息系统索引内部业务的唯一编号，其作用包括但不限于：用于本地存证系统或中心存证系统溯源取证时进行高效检索存证对象，本专利对其作用不做具体约束；

第一存证对象的大小用于表示第一存证对象内容的大小，表示方式包括但不限于字节；

第一存证对象内容的描述是对第一存证对象的内容的简要描述；

待生成的存证请求内容完整性的度量值及签名中的完整性的度量值是指信息系统对待生成的存证请求内容进行变换得到的值，确保待生成的存证请求内容的完整性，签名是指信息系统对待生成的存证请求内容进行签名，确保不可抵赖性。

基于上述任一实施例，步骤 140 中，所述基于所述认证校验码生成第一存证消息，包括：

基于信息系统标识和第二存证对象的认证校验码，生成第一存证消息；

或者，

基于信息系统标识和第二存证对象的认证校验码，以及所述第一存证对象的操作主体、第一存证对象的操作行为、协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统的网络地址、信息系统的硬件地址、存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、密文字段和待生成的第一存证消息完整性的度量值及签名中的至少一种，生成第一存证消息。

具体地，可以基于信息系统标识和第二存证对象的认证校验码生

成第一存证消息。即第一存证消息中，可以包括信息系统标识和第二存证对象的认证校验码。

除此以外，还可以基于信息系统标识和第二存证对象的认证校验码，以及所述第一存证对象的操作主体、第一存证对象的操作行为、协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统的网络地址、信息系统的硬件地址、存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、密文字段和待生成的第一存证消息完整性的度量值及签名中的至少一种，生成第一存证消息。

即，第一存证消息中，可以包括信息系统标识和第二存证对象的认证校验码，还可以包括第一存证对象的操作主体、第一存证对象的操作行为、协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统的网络地址、信息系统的硬件地址、存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、密文字段、待生成的第一存证消息完整性的度量值及签名中的至少一种。为便于说明，以下将第一存证消息记为 D_3。

将所述信息系统标识和第二存证对象的认证校验码，记为待生成的第一存证消息内容；

或者，

所述信息系统标识和第二存证对象的认证校验码，以及所述信息系统的网络地址、信息系统的硬件地址、存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果和密文字段，记为待生成的第一存证消息内容。

需要说明的是，不同的信息系统可以在数据包 D_3 中的第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号上有所区分，由此表示不同版本的信息内容。

其中，第一存证对象的操作主体包括但不限于第一存证对象的操作自然人、组织、设备或程序等实体，本专利不作具体约束；

第一存证对象的操作行为包括但不限于：发送文件、查阅文件、审批文件、下载文件、删除文件、分类分级、分类分级效果评估、脱敏、脱敏效果评估、删除、删除效果评估、异常信息处置等，本专利不作具体约束；

存证系统的业务内部索引号此处是指本地存证系统业务内部索引号，用于索引本地存证系统内部业务的唯一编号，其作用包括但不限于：用于中心存证系统溯源取证时进行高效检索信息系统的业务内部索引号，本地存证系统的业务内部索引号和信息系统的业务内部索引号是一一对应的，本专利对其作用不做具体约束；

第一存证对象内容的描述是指第一存证对象内容的简要描述；

第一存证对象内容的检索词是指查询第一存证对象内容的关键

字；

第一存证对象的分类号是指第一存证对象内容的分类；

第一存证对象的所属主体是指第一存证对象的所属自然人、组织、设备或程序等实体，本专利不作具体约束；

第一存证对象的创建时间是指第一存证对象的创建的时刻，格式不限，例如“yyyy-MM-dd HH:mm:ss”；

第一存证对象的创建地点是指第一存证对象的被创建所在的位置，格式不限，例如经纬度表示法；

第一存证对象的操作时间是指第一存证对象的被操作的时刻，格式不限，例如“yyyy-MM-dd HH:mm:ss”；

第一存证对象的操作位置是指第一存证对象的被操作所在的位置，格式不限，例如经纬度表示法；

第一存证对象的操作结果是指第一存证对象被操作变化后的存证对象；

密文字段是接收存证系统返回的存证请求应答中的字段，由信息系统直接发送至本地存证系统，信息系统不进行任何操作；

待生成的第一存证消息的完整性的度量值及签名中的完整性的度量值是指信息系统对待生成的第一存证消息内容进行变换得到的值，确保待生成的存证请求内容的完整性，签名是信息系统对待生成的第一存证消息内容进行签名，确保不可抵赖性。

基于上述任一实施例，用于进行存证的存证系统可以包括中心存证系统和本地存证系统。

中心存证系统、本地存证系统与信息系统三者之间可以是一对一关系，也可以是多对多关系。即，本地存证系统可以多层进行部署，同层之间也可以部署多个，例如：本地存证系统部署方式分为国家级（美国节点、中国节点）、省市级（同层可分为北京市本地存证系统、河北省本地存证系统、纽约州本地存证系统等等）、每个省级节点下

包括具体的本地存证节点，本地存证节点可以部署在信息系统所在单位处，用于存储和管理信息系统的各种操作，记录数据的流转状态；中心存证系统可以多层部署，同层之间也可以部署多个，例如：中心存证系统部署方式分为国家级、省市级（同层可分为北京市中心存证系统、河北省中心存证系统等等），中心存证系统用于存储和管理各级本地存证系统或信息系统上报的关键存证信息字段。具体地，此部署架构是可变的，可以是多层级部署，每层级可以部署多个；也可以单层级部署，本专利对部署的架构不做具体约束，不同的部署架构均属于本专利的保护范围。

在上述架构下，步骤 110 中，所述将所述存证请求发送到存证系统，包括：

将所述存证请求直接发送至所述中心存证系统，或者，将所述存证请求发送至所述本地存证系统，以使所述本地存证系统将所述存证请求发送至所述中心存证系统；

具体地，信息系统可以直接与中心存证系统通信，即，信息系统可以直接将存证请求发送到中心存证系统；或者，信息系统也可以通过本地存证系统发送，以实现与中心存证系统之间的通信，即，信息系统可以将存证请求发送到本地存证系统，再由本地存证系统将接收到的存证请求发送到中心存证系统。

相应地，步骤 120 中，所述接收所述存证系统返回的存证请求应答，包括：

接收所述中心存证系统直接返回的存证请求应答，或者，接收所述中心存证系统返回并经过所述本地存证系统发送的存证请求应答。

具体地，中心存证系统可以直接与信息系统通信，即，中心存证系统可以直接将存证请求应答发送到信息系统；或者，中心存证系统也可以通过本地存证系统发送，以实现与信息系统之间的通信，即，中心存证系统可以将存证请求应答发送到本地存证系统，再由本地存

证系统将接收到的存证请求应答发送到信息系统。

基于上述任一实施例，步骤 140 中，所述将所述第一存证消息发送到所述存证系统进行存证，包括：

所述第一存证消息直接发送所述中心存证系统，中心存证系统基于所述第一存证消息向所述信息系统返回第二存证收条，包括：

将所述第一存证消息直接发送所述中心存证系统，中心存证系统基于所述第一存证消息向所述信息系统返回第二存证收条；或者，将所述第一存证消息发送到所述本地存证系统，以使所述本地存证系统基于所述第一存证消息生成第二存证消息，并将所述第二存证消息发送至所述中心存证系统，所述中心存证系统基于所述第二存证消息向所述本地存证系统返回第二存证收条；

接收所述本地存证系统基于所述第二存证收条返回的第一存证收条。

具体地，需要结合中心存证系统和本地存证系统进行存证。信息系统可以将第一存证消息发送到本地存证系统，本地存证系统在接收到第一存证消息之后，可以生成第二存证消息。此处的第二存证消息同样可以包括第一存证消息中的第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号。本地存证系统可以将第二存证消息发送到中心存证系统，以告知中心存证系统自身接收到了第一存证消息，进行存证报备。

中心存证系统可以在接收到第二存证消息之后，返回第二存证收条到本地存证系统。本地存证系统在接收到第二存证收条之后，确认存证报备完成，再向信息系统返回第一存证收条。

信息系统在接收到第一存证收条之后，确认存证完成。

或者，

信息系统也可以将第一存证消息直接发送到中心存证系统，中心

存证系统在接收到第一存证消息之后，返回第二存证收条到信息系统。

信息系统在接收到第二存证收条之后，确认存证完成。

基于上述任一实施例，图 2 是本发明提供的存证方法的流程示意图之二，如图 2 所示，该方法应用于存证系统，该方法包括：

步骤 210，接收信息系统发送的存证请求，所述存证请求与第一存证对象对应。

此处，信息系统即证据发送方，也就是需要进行信息存证的一方。第一存证对象即存证对象待存证的原始信息。相应地，存证系统即信息存证方，也就是用于实现信息存证的一方。

信息系统在确定第一存证对象之后，即可对应生成存证请求，并将存证请求发送到存证系统。可以理解的是，第一存证对象与存证请求一一对应，存证请求中携带了第一存证对象的相关信息，例如第一存证对象的类型、第一存证对象的大小和第一存证对象的内容描述等，本发明实施例对此不作具体限定。

相应地，存证系统可以接收信息系统发送的存证请求。

步骤 220，获取与所述存证请求对应的存证请求应答。

步骤 230，将所述存证请求应答返回到所述信息系统，以使所述信息系统基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码，并基于所述认证校验码生成第一存证消息。

具体地，存证系统在接收到存证请求之后，即可获取与存证请求对应的存证请求应答。此处获取存证请求应答，具体可以是生成存证请求应答，也可以是接收其他存证系统发送的存证请求应答。例如当存证系统为中心存证系统时，可以直接生成存证请求应答。又例如当存证系统为本地存证系统时，可以将存证请求发送到中心存证系统，并接收中心存证系统返回的存证请求应答。

在获取到存证请求应答之后，即可将存证请求应答返回到信息系统。

此处的存证请求应答中携带有随机内容插入规则和随机内容。

信息系统在接收到存证请求应答之后，即可从中获取到随机内容插入规则和随机内容，并基于此两者，生成对第一存证对象进行存证所需的认证校验码。

在此过程中，信息系统需要基于存证请求应答中的随机内容插入规则，将存证请求应答中的随机内容插入到第一存证对象中，由此得到第二存证对象。可以理解的是，此处的第二存证对象即在第一存证对象中、在随机内容插入规则所指示的位置处插入了随机对象之后的存证对象。

在得到第二存证对象之后，即可针对第二存证对象进行变换，并将变换所得的结果，作为第二存证对象的认证校验码。

可以理解的是，相较于直接针对第一存证对象进行变换所得的认证校验码，本发明实施例中基于随机内容插入规则、将随机内容插入第一存证对象后再进行变换得到的认证校验码，通过伪造生成具有相同语义且相同类型的存证对象理论上不可能，可以有效避免有意伪造存证对象的情况发生。

信息系统在得到第二存证对象的认证校验码之后，即可生成携带该认证校验码的第一存证消息，并将第一存证消息返回到存证系统。

步骤 240，基于所述信息系统发送的第一存证消息进行存证。

相应地，存证系统可以接收信息系统发送的第一存证消息，并基于此进行存证。

本发明实施例提供的方法，基于第一存证对象的类型生成随机内容和随机内容插入规则，将随机内容按照随机内容插入规则插入到第一存证对象生成第二存证对象、再对第二存证对象进行变换获取第二存证对象的认证校验码，由于随机内容插入规则和随机内容是存证系

统根据对象的类型进行生成、且不可变更，认证校验码具有机密性、完整性和数据源认证的特性，因此通过伪造生成具有相同语义且相同类型的存证对象理论上不可能，可以有效避免有意伪造存证对象的情况发生。存证系统存储基于第二存证对象的认证校验码生成的存证消息（仅包含认证校验码和相关管理信息），不存储存证对象的内容，既保护了存证对象的内容，消除了数据泄露的风险，还大幅度降低了数据传输带宽和存证系统的存储开销。存证消息中的业务内部索引号提升了在溯源取证过程中索引存证对象的效率。存证信息上报采用加密方式传输，保障了存证信息传输过程中的安全。本专利在抗数据伪造与泄露、降低传输带宽和存储开销、提高存储效率和证据检索效率等方面具有显著的优势，提高了存证的可信度与效率。

基于上述任一实施例，步骤220中，所述获取与所述存证请求对应的存证请求应答，包括：

基于所述存证请求中所述第一存证对象的类型，确定所述随机内容插入规则；

或者，

基于所述存证请求中所述第一存证对象的类型，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统标识、信息系统的网络地址、信息系统的硬件地址、信息系统的业务内部索引号、第一存证对象的大小、第一存证对象内容的描述和存证请求内容完整性的度量值及签名中的至少一种，确定所述随机内容插入规则；

生成所述随机内容；

基于所述随机内容插入规则和所述随机内容，生成与所述存证请求对应的存证请求应答。

具体地，存储请求中包括第一存证对象的类型。

存证系统在得到存证请求后，可以基于存证请求中携带的第一存

证对象的类型，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统标识、信息系统的网络地址、信息系统的硬件地址、信息系统的业务内部索引号、第一存证对象的大小、第一存证对象内容的描述和存证请求内容完整性的度量值及签名中的至少一种，为第一存证对象生成对应的随机内容插入规则。此处，随机内容插入规则可以是预先设定好的，例如可以根据第一存证对象的类型，确定将随机内容放在文件头部、尾部，或者放在第一存证对象大小字节范围的任意预设字节处，本发明实施例对此不作具体限定。

此外，可以基于一定方法生成随机内容。

在得到随机内容插入规则和随机内容之后，即可生成携带有此两者的存证请求应答。

基于上述任一实施例，步骤 220 中，所述基于所述随机内容插入规则和所述随机内容，生成与所述存证请求对应的存证请求应答，包括：

基于所述随机内容插入规则和所述随机内容，生成与所述存证请求对应的存证请求应答；

或者，

基于所述随机内容插入规则和所述随机内容，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、存证系统标识、存证系统的业务内部索引号、信息系统的业务内部索引号、请求应答时间、密文字段和待生成的存证请求应答内容完整性的度量值及签名中的至少一种，生成与所述存证请求对应的存证请求应答。

具体地，可以基于所述随机内容插入规则和所述随机内容，生成与存证请求对应的存证请求应答。即，存证请求应答中，可以包括所述随机内容插入规则和所述随机内容。

除此以外，还可以基于随机内容插入规则和所述随机内容，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、存证系统标识、存证系统的业务内部索引号、信息系统的业务内部索引号、请求应答时间、密文字段和待生成的存证请求应答内容完整性的度量值及签名中的至少一种，生成与所述存证请求对应的存证请求应答。

即，存证请求应答中，可以包括随机内容插入规则和所述随机内容，还可以包括协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、存证系统标识、存证系统的业务内部索引号、信息系统的业务内部索引号、请求应答时间、密文字段和待生成的存证请求应答内容完整性的度量值及签名中的至少一种。为便于说明，以下将存证请求应答记为 D_2。

将所述随机内容插入规则和所述随机内容，记为待生成的存证请求应答内容；

或者，

将所述随机内容插入规则和所述随机内容，以及所述存证系统标识、存证系统的业务内部索引号和请求应答时间中的至少一种，记为待生成的存证请求应答内容。

进一步地，存证请求应答由中心存证系统生成，此存证请求应答中的存证系统标识为中心存证系统标识，中心存证系统标识用于区分不同的中心存证系统，存证系统的业务内部索引号为中心存证系统的业务内部索引号；

中心存证系统的业务内部索引号是中心存证系统索引内部业务的唯一编号，其作用包括但不限于：在溯源取证时进行高效检索本地存证系统的业务内部索引号或者信息系统的业务内部索引号，中心存证系统的业务内部索引号和本地存证系统的业务内部索引号以及中心存证系统的业务内部索引号和信息系统的业务内部索引号均是一

一对应的，本专利对其作用不做具体约束；

密文字段包括但不限于由时间戳、随机数和固定字符串的组合后的加密文本，此阶段由中心存证系统返回给信息系统；

请求应答时间是用于表示中心存证系统反馈存证请求应答的具体时刻；格式不限，例如 “yyyy-MM-dd HH:mm:ss”；

待生成的存证请求应答内容完整性的度量值及签名中的完整性的度量值是指中心存证系统对待生成的存证请求应答内容进行变换得到的值，确保待生成的存证请求内容的完整性，签名是中心存证系统对待生成的存证请求应答内容进行签名，确保不可抵赖性。

基于上述任一实施例，所述存证系统包括中心存证系统和本地存证系统。

本地存证系统可以多层进行部署，同层之间也可以部署多个，例如：本地存证系统部署方式分为国家级（美国节点、中国节点）、省市级（同层可分为北京市本地存证系统、河北省本地存证系统、纽约州本地存证系统等等）、每个省级节点下包括具体的本地存证节点，本地存证节点可以部署在信息系统所在单位处，用于存储和管理信息系统的各种操作，记录数据的流转状态；中心存证系统可以多层部署，同层之间也可以部署多个，例如：中心存证系统部署方式分为国家级、省市级（同层可分为北京市中心存证系统、河北省中心存证系统等等），中心存证系统用于存储和管理各级本地存证系统或信息系统上报的关键存证信息字段。

在上述架构下，在上述存证方法应用于中心存证系统的情况下，步骤 240 中，所述基于所述信息系统发送的存证消息进行存证，包括：

接收所述信息系统直接发送的第一存证消息，生成第二存证收条并直接返回至所述信息系统；

或者，

接收所述本地存证系统发送的第二存证消息，生成第二存证收条

返回至所述本地存证系统，以使所述本地存证系统在接收到所述第二存证收条后生成第一存证收条，并将所述第一存证收条返回至所述信息系统，或者通过所述本地存证系统所述第二存证收条发送至所述信息系统，所述第二存证消息是所述本地存证系统基于所述第一存证消息生成的。

基于中心存证系统标识，生成第二存证收条并直接返回至所述信息系统；

或者，

基于中心存证系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、信息系统标识、信息系统的网络地址、信息系统的硬件地址、中心存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的类型、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作结果、第二存证对象的认证校验码、密文字段、第一存证消息完整性的度量值及签名和待生成的第二存证收条完整性的度量值及签名中的至少一种，生成第二存证收条并直接返回至所述信息系统。

具体地，可以基于中心存证系统标识，生成第二存证收条，即，第二存证收条中，包括中心存证系统标识。

除此以外，还可以基于中心存证系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、信息系统标识、信息系统的网络地址、信息系统的硬件地址、中心存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象内容的标题、第一存证对

象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的类型、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作结果、第二存证对象的认证校验码、密文字段、第一存证消息完整性的度量值及签名和待生成的第二存证收条完整性的度量值及签名中的至少一种，生成第二存证收条；

即，第二存证收条可以包括中心存证系统标识，还可以包括协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、信息系统标识、信息系统的网络地址、信息系统的硬件地址、中心存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的类型、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作结果、第二存证对象的认证校验码、密文字段、第一存证消息完整性的度量值及签名和待生成的第二存证收条完整性的度量值及签名中的至少一种。为便于说明，以下将第二存证收条记为 D_5。

将所述第二存证收条标识，记为待生成的第二存证收条；

或者，

将所述第二存证收条标识，以及所述中心存证系统标识、第二存证收条时间、中心存证系统的业务内部索引号和信息系统的业务内部索引号中的至少一种，记为待生成的第二存证收条。

其中，第二存证收条标识是指中心存证系统用于反馈已接收到上报的第一存证消息，在中心存证系统中第二存证收条标识均是唯一的，

用于区分上报的第一存证消息，直接由中心存证系统返回至信息系统；

第二存证收条时间是中心存证系统对收到第一存证消息的反馈时刻，格式不限；

此处的待生成的第二存证收条完整性的度量值及签名中的完整性的度量值是指中心存证系统对待生成的第二存证收条进行变换得到的值，确保待生成的第二存证收条的完整性，签名是中心存证系统对待生成的第二存证收条进行签名，确保不可抵赖性。

基于中心存证系统标识，生成第二存证收条返回至所述本地存证系统；

或者，

基于中心存证系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、信息系统标识、中心存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第二存证对象的认证校验码、第一存证消息完整性的度量值及签名、第二存证消息完整性的度量值及签名和待生成的第二存证收条完整性的度量值及签名中的至少一种，生成第二存证收条返回至所述本地存证系统。

具体地，可以基于中心存证系统标识，生成第二存证收条，即，第二存证收条中，包括中心存证系统标识。

除此以外，还可以基于中心存证系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、信息系统标识、中心存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第二存证对象的认证

校验码、第一存证消息完整性的度量值及签名、第二存证消息完整性的度量值及签名和待生成的第二存证收条完整性的度量值及签名中的至少一种，生成第二存证收条；

即，第二存证收条包括中心存证系统标识，还可以包括协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、信息系统标识、中心存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的大小、第一存证对象内容的标题、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第二存证对象的认证校验码、第一存证消息完整性的度量值及签名、第二存证消息完整性的度量值及签名和待生成的第二存证收条完整性的度量值及签名中的至少一种。为便于说明，以下将第二存证收条记为 D_5。

将所述第二存证收条标识，记为待生成的第二存证收条；

或者，

将所述第二存证收条标识，以及所述中心存证系统标识、第二存证收条时间、中心存证系统的业务内部索引号和信息系统的业务内部索引号中的至少一种，记为待生成的第二存证收条。

其中，第二存证收条标识是指中心存证系统用于反馈已接收到上报的第二存证消息，在中心存证系统中第二存证收条标识均是唯一的，用于区分上报的第二存证消息，直接由中心存证系统返回至信息系统；

第二存证收条时间是中心存证系统对收到第二存证消息的反馈时刻，格式不限；

此处的待生成的第二存证收条完整性的度量值及签名中的完整性的度量值是指中心存证系统对待生成的第二存证收条进行变换得到的值，确保待生成的第二存证收条的完整性，签名是中心存证系统对待生成的第二存证收条进行签名，确保不可抵赖性。

基于上述任一实施例，在上述架构下，在上述存证方法应用于本

地存证系统的情况下，步骤240中，所述基于所述信息系统发送的存证消息进行存证，包括：

接收所述第一存证消息，并基于所述信息系统标识生成第二存证消息；

或者，

接收所述第一存证消息，并基于信息系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统的网络地址、信息系统的硬件地址、本地存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、第一存证消息完整性的度量值及签名和待生成的第二存证消息完整性的度量值及签名中的至少一种，生成第二存证消息；

将所述第二存证消息发送至所述中心存证系统，以使所述中心存证系统在接收到所述第二存证消息后生成第二存证收条；

在接收到所述中心存证系统返回的第二存证收条后，生成第一存证收条返回所述信息系统。

具体地，在该方法应用于本地存证系统的情况下，信息系统将第一存证消息发送到本地存证系统，本地存证系统即可基于第一存证消息生成第二存证消息，并将第二存证消息发送到中心存证系统。为便于说明，以下将第二存证消息记为 D_4。

将信息系统标识记为待生成的第二存证消息；

或者，

将信息系统标识，以及信息系统的网络地址、信息系统的硬件地址、本地存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第二存证对象的认证校验码和第一存证消息完整性的度量值及签名记为待生成的第二存证消息。

具体地，可以基于信息系统标识生成第二存证消息。即，第二存证消息包括信息系统标识。

除此以外，本地存证系统还可以基于信息系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统的网络地址、信息系统的硬件地址、本地存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象内容的描述、第一存证对象的大小、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、第一存证消息完整性的度量值及签名和待生成的第二存证消息完整性的度量值及签名中的至少一种，生成第二存证消息 D_4。

即，第二存证消息 D_4 中除了可以包括信息系统标识，还可以包括协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统的网络地址、信息系统的硬件地址、本地存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一

存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、第一存证消息完整性的度量值及签名和待生成的第二存证消息完整性的度量值及签名中的至少一种。

其中，第一存证消息完整性的度量值及签名中的完整性的度量值是指信息系统对第一存证消息进行变换得到的值，确保第一存证消息的完整性，签名是信息系统对第一存证消息进行签名，确保不可抵赖性。

待生成的第二存证消息完整性的度量值及签名中的完整性的度量值是指本地存证系统对待生成的第二存证消息进行变换得到的值，确保待生成的第二存证消息的完整性，签名是本地存证系统对待生成的第二存证消息进行签名，确保不可抵赖性。

基于本地存证系统标识，生成第一存证收条返回所述信息系统；

或者，

基于本地存证系统标识，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、第一存证收条标识、第一存证收条时间、信息系统标识、信息系统的网络地址、信息系统的硬件地址、中心存证系统的业务内部索引号、本地存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、密文字段、第一存证消息完整性的度量值及签名、第

二存证消息完整性的度量值及签名、第二存证收条完整性的度量值及签名和待生成的第一存证收条完整性的度量值及签名中的至少一种，生成第一存证收条返回所述信息系统；

本地存证系统在生成第二存证消息之后，即可将第二存证消息发送到中心存证系统，中心存证系统在接收到第二存证消息之后，即可据此生成第二存证收条并返回本地存证系统。

本地存证系统在收到第二存证收条之后，即可基于本地存证系统标识，生成第一存证收条。即，第一存证收条包括本地存证系统标识，为便于说明，以下将第一存证收条记为 D_6。

除此以外，还可以基于本地存证系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、第一存证收条标识、第一存证收条时间、信息系统标识、信息系统的网络地址、信息系统的硬件地址、中心存证系统的业务内部索引号、本地存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、密文字段、第一存证消息完整性的度量值及签名、第二存证消息完整性的度量值及签名、第二存证收条完整性的度量值及签名和待生成的第一存证收条完整性的度量值及签名中的至少一种，生成第一存证收条。

即，第一存证收条可以包括本地存证系统标识，还可以包括协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、第一存证收条标

识、第一存证收条时间、信息系统标识、信息系统的网络地址、信息系统的硬件地址、中心存证系统的业务内部索引号、本地存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、密文字段、第一存证消息完整性的度量值及签名、第二存证消息完整性的度量值及签名、第二存证收条完整性的度量值及签名和待生成的第一存证收条完整性的度量值及签名中的至少一种。

将第一存证收条标识，记为待生成的第一存证收条；

或者，

将第一存证收条标识，以及本地存证系统标识、第一存证收条时间、中心存证系统的业务内部索引号、信息系统的业务内部索引号记为待生成的第一存证收条。

其中，待生成的第一存证收条完整性的度量值及签名中的完整性的度量值是指本地存证系统对待生成的第一存证收条进行变换得到的值，确保待生成的第一存证收条的完整性，签名是本地存证系统对待生成的第一存证收条进行签名，确保不可抵赖性。

在生成第一存证收条之后，即可将第一存证收条返回到信息系统。此处，是否需要生成第一存证收条并返回信息系统，取决于本地存证系统和信息系统是否部署在同一单位。进一步地，如果本地存证系统和信息系统部署在同一单位，则可以省略本地存证系统向信息系统反馈第一存证收条的步骤。而如果本地存证系统下部署有多家信息系统，则需要本地存证系统向信息系统反馈第一存证收条。

此处，其中第一存证收条可以与第二存证收条相同，也可以比第二存证收条多，也可以比第二存证收条少，本专利不做限制。

基于上述任一实施例，图 3 是本发明提供的存证方法的流程示意图之三，如图 3 所示，该方法包括：

S1、信息系统 A 向中心存证系统 B 发送存证请求：

信息系统 A 可以针对第一存证对象生成存证请求 D_1，并将存证请求 D_1 发送到中心存证系统 B。

S2、中心存证系统 B 向信息系统 A 返回存证请求应答：

中心存证系统 B 在接收到存证请求 D_1 之后，可以生成存证请求应答 D_2，并将存证请求应答 D_2 返回到信息系统 A。

S3、信息系统 A 向本地存证系统 C 上报第一存证消息：

信息系统 A 可以基于存证请求应答 D_2 中的随机内容插入规则，将存证请求应答 D_2 中的随机内容插入第一存证对象，得到第二存证对象，并对第二存证对象进行变换，得到第二存证对象的认证校验码，由此生成携带认证校验码的第一存证消息 D_3，并将第一存证消息 D_3 上报本地存证系统 C。

S3’、信息系统 A 向中心存证系统 B 直接上报第一存证消息：

信息系统 A 可以基于存证请求应答 D_2 中的随机内容插入规则，将存证请求应答 D_2 中的随机内容插入第一存证对象，得到第二存证对象，并对第二存证对象进行变换，得到第二存证对象的认证校验码，由此生成携带认证校验码的第一存证消息 D_3，并将第一存证消息 D_3 上报中心存证系统 B。

S4、本地存证系统 C 向中心存证系统 B 上报第二存证消息：

本地存证系统 C 在收到第一存证消息 D_3 之后，生成第二存证消息 D_4，并将第二存证消息 D_4 上报中心存证系统 B。

S5、中心存证系统 B 向本地存证系统 C 反馈第二存证收条：

中心存证系统 B 在收到第二存证消息 D_4 之后，生成第二存证收

条 D_5，并将第二存证收条 D_5 反馈到本地存证系统 C。

S5’、中心存证系统 B 向信息系统 A 直接反馈第二存证收条：

中心存证系统 B 在收到第一存证消息 D_3 之后，生成第二存证收条 D_5，并将第二存证收条 D_5 直接反馈到信息系统 A。

S6、本地存证系统 C 向信息系统 A 反馈第一存证收条：

本地存证系统 C 在收到第二存证收条 D_5 之后，生成第一存证收条 D_6，并将第一存证收条 D_6 反馈到信息系统 A。

基于上述任一实施例，图 4 是本发明提供的存证方法的流程示意图之四，如图 4 所示，信息系统 A 可以包括各种类型的信息系统，例如分类分级相关系统 A1、脱敏相关系统 A2、删除相关系统 A3、监管相关系统 A4 等。

进一步地，分类分级相关系统 A1 可以包括个人敏感信息识别系统，该系统对应本地存证系统 C1，以及分类分级效果测评系统，该系统对应本地存证系统 C2。

脱敏相关系统 A2 可以包括个人信息拆分脱敏存储与重构系统，该系统对应本地存证系统 C3，以及脱敏效果测评系统，该系统对应本地存证系统 C4。

删除相关系统 A3 可以包括确定性删除系统，该系统对应本地存证系统 C5，以及删除指令通知与确认系统，该系统对应本地存证系统 C6。

监管相关系统 A4 可以包括权益保障监管与处置系统，该系统对应本地存证系统 C7，此外还可以包括对应本地存证系统 C8 的其他系统。

各个本地存证系统可以与隐私数据流转状态管理与存证系统，也就是中心存证系统 B 相互通信。此外，信息系统 A 也可以直接与中心存证系统 B 相互通信。

在此架构下，存证方法的步骤包括：

① 信息系统 A 向中心存证系统 B 发送存证请求；

② 中心存证系统 B 向信息系统 A 返回存证请求应答；

③ 信息系统 A 向本地存证系统 C 发送第一存证消息；

④ 本地存证系统 C 向中心存证系统 B 发送第二存证消息；

⑤ 中心存证系统 B 向本地存证系统 C 返回第二存证收条；

⑥ 本地存证系统 C 向信息系统 A 返回第一存证收条。

在此架构下，中心存证系统对数据管理、存储、查询等方面的压力得到了缓解，提高了整体系统的性能。

通过设计分布式存证架构，大幅度降低了中心存证系统服务的负载，将数据组织、管理、检索下载等功能下放到本地存证系统服务中，提升了中心存证系统的高并发性和高可用性；业务层面上，通过中心存证系统的监管服务，依据存证信息可以对侵权行为做到全域追踪溯源。

基于上述任一实施例，图 5 是本发明提供的存证方法的流程示意图之四，如图 5 所示，中心存证系统与本地存证系统是一对多的通信关系，中心存证系统与信息系统是一对多的通信关系，本地存证系统与信息系统是一对多的通信关系。

在此架构下，存证方法的步骤包括：

①；

通过设计多层级的部署架构，大幅度降低了国家级和省市级中心存证系统服务的负载，将数据内容的组织、管理、检索等功能下放到各级本地存证系统服务中，提升了国家级和省市级中心存证系统的高并发性和高可用性；业务层面上，通过中心存证系统的监管服务，依据存证信息可以对侵权行为做到全域追踪溯源。

基于上述任一实施例，图 6 是本发明提供的存证装置的结构示意图之一，如图 6 所示，该存证装置可以应用于信息系统，该存证装置包括：

请求发送单元610，用于确定第一存证对象，生成所述第一存证对象对应的存证请求，并将所述存证请求发送到存证系统；

应答接收单元620，用于接收所述存证系统返回的存证请求应答；

认证校验码生成单元630，用于基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，并对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码；

存证发送单元640，用于基于所述认证校验码生成第一存证消息，并将所述第一存证消息发送到所述存证系统进行存证。

本发明实施例提供的方法，基于第一存证对象的类型生成随机内容和随机内容插入规则，将随机内容按照随机内容插入规则插入到第一存证对象生成第二存证对象、再对第二存证对象进行变换获取第二存证对象的认证校验码，由于随机内容插入规则和随机内容是存证系统根据对象的类型进行生成、且不可变更，认证校验码具有机密性、完整性和数据源认证的特性，因此通过伪造生成具有相同语义且相同类型的存证对象理论上不可能，可以有效避免有意伪造存证对象的情况发生。存证系统存储基于第二存证对象的认证校验码生成的存证消息（仅包含认证校验码和相关管理信息），不存储存证对象的内容，既保护了存证对象的内容，消除了数据泄露的风险，还大幅度降低了数据传输带宽和存证系统的存储开销。存证消息中的业务内部索引号提升了在溯源取证过程中索引存证对象的效率。存证信息上报采用加密方式传输，保障了存证信息传输过程中的安全。本专利在抗数据伪造与泄露、降低传输带宽和存储开销、提高存储效率和证据检索效率等方面具有显著的优势，提高了存证的可信度与效率。

基于上述任一实施例，请求发送单元具体用于：

基于所述第一存证对象的类型，生成所述第一存证对象对应的存证请求；

或者，

基于所述第一存证对象的类型，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统标识、信息系统的网络地址、信息系统的硬件地址、信息系统的业务内部索引号、第一存证对象的大小、第一存证对象内容的描述和待生成的存证请求内容完整性的度量值及签名中的至少一种，生成所述第一存证对象对应的存证请求。

基于上述任一实施例，存证发送单元具体用于：

基于信息系统标识和第二存证对象的认证校验码，生成第一存证消息；

或者，

基于信息系统标识和第二存证对象的认证校验码，以及所述第一存证对象的操作主体、第一存证对象的操作行为、协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统的网络地址、信息系统的硬件地址、存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、密文字段和待生成的第一存证消息完整性的度量值及签名中的至少一种，生成第一存证消息。

基于上述任一实施例，所述存证系统包括中心存证系统和本地存证系统；

所述请求发送单元具体用于：

将所述存证请求直接发送至所述中心存证系统，或者，将所述存证请求发送至所述本地存证系统，以使所述本地存证系统将所述存证

请求发送至所述中心存证系统；

所述应答接收单元具体用于：

接收所述中心存证系统直接返回的存证请求应答，或者，接收所述中心存证系统返回并经过所述本地存证系统发送的存证请求应答。

基于上述任一实施例，存证发送单元具体用于：

将所述第一存证消息发送到所述本地存证系统，以使所述本地存证系统基于所述第一存证消息生成第二存证消息，并将所述第二存证消息发送至所述中心存证系统，所述中心存证系统基于所述第二存证消息向所述本地存证系统返回第二存证收条；

接收所述本地存证系统基于所述第二存证收条返回的第一存证收条。

基于上述任一实施例，图 7 是本发明提供的存证装置的结构示意图之二，如图 7 所示，该存证装置可以应用于存证系统，该存证装置包括：

请求接收单元 710，用于接收信息系统发送的存证请求，所述存证请求与第一存证对象对应；

应答获取单元 720，用于获取与所述存证请求对应的存证请求应答；

应答返回单元 730，用于将所述存证请求应答返回到所述信息系统，以使所述信息系统基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码，并基于所述认证校验码生成第一存证消息；

存证单元 740，用于基于所述信息系统发送的第一存证消息进行存证。

本发明实施例提供的方法，基于第一存证对象的类型生成随机内容和随机内容插入规则，将随机内容按照随机内容插入规则插入到第

一存证对象生成第二存证对象、再对第二存证对象进行变换获取第二存证对象的认证校验码，由于随机内容插入规则和随机内容是存证系统根据对象的类型进行生成、且不可变更，认证校验码具有机密性、完整性和数据源认证的特性，因此通过伪造生成具有相同语义且相同类型的存证对象理论上不可能，可以有效避免有意伪造存证对象的情况发生。存证系统存储基于第二存证对象的认证校验码生成的存证消息（仅包含认证校验码和相关管理信息），不存储存证对象的内容，既保护了存证对象的内容，消除了数据泄露的风险，还大幅度降低了数据传输带宽和存证系统的存储开销。存证消息中的业务内部索引号提升了在溯源取证过程中索引存证对象的效率。存证信息上报采用加密方式传输，保障了存证信息传输过程中的安全。本专利在抗数据伪造与泄露、降低传输带宽和存储开销、提高存储效率和证据检索效率等方面具有显著的优势，提高了存证的可信度与效率。

基于上述任一实施例，应答获取单元具体用于：

基于所述存证请求中所述第一存证对象的类型，确定所述随机内容插入规则；

或者，

基于所述存证请求中所述第一存证对象的类型，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统标识、信息系统的网络地址、信息系统的硬件地址、信息系统的业务内部索引号、第一存证对象的大小、第一存证对象内容的描述和存证请求内容完整性的度量值及签名中的至少一种，确定所述随机内容插入规则；

生成所述随机内容；

基于所述随机内容插入规则和所述随机内容，生成与所述存证请求对应的存证请求应答。

基于上述任一实施例，应答获取单元具体用于：

基于所述随机内容插入规则和所述随机内容，生成与所述存证请求对应的存证请求应答；

或者，

基于所述随机内容插入规则和所述随机内容，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、存证系统标识、存证系统的业务内部索引号、信息系统的业务内部索引号、请求应答时间、密文字段和待生成的存证请求应答内容完整性的度量值及签名中的至少一种，生成与所述存证请求对应的存证请求应答。

基于上述任一实施例，所述存证系统包括中心存证系统和本地存证系统，在所述存证装置应用于所述中心存证系统的情况下，所述存证单元具体用于：

接收所述本地存证系统发送的第二存证消息，所述第二存证消息是所述本地存证系统基于所述第一存证消息生成的；

接收所述信息系统直接发送的第一存证消息，生成第二存证收条并直接返回至所述信息系统；

或者，

接收所述本地存证系统发送的第二存证消息，生成第二存证收条返回至所述本地存证系统，以使所述本地存证系统在接收到所述第二存证收条后生成第一存证收条，并将所述第一存证收条返回至所述信息系统，或者通过所述本地存证系统所述第二存证收条发送至所述信息系统，所述第二存证消息是所述本地存证系统基于所述第一存证消息生成的。

基于中心存证系统标识，生成第二存证收条并直接返回至所述信息系统；

或者，

基于中心存证系统标识，以及协议版本号、命令类别、存证事项

类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、信息系统标识、信息系统的网络地址、信息系统的硬件地址、中心存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的类型、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、密文字段、第一存证消息完整性的度量值及签名和待生成的第二存证收条完整性的度量值及签名中的至少一种，生成第二存证收条并直接返回至所述信息系统。

基于中心存证系统标识，生成第二存证收条返回至所述本地存证系统；

或者，

基于中心存证系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、信息系统标识、中心存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第二存证对象的认证校验码、第一存证消息完整性的度量值及签名、第二存证消息完整性的度量值及签名和待生成的第二存证收条完整性的度量值及签名中的至少一种，生成第二存证收条返回至所述本地存证系统。

基于上述任一实施例，所述存证系统包括中心存证系统和本地存证系统，在所述存证装置应用于所述本地存证系统的情况下，所述存证单元具体用于：

接收所述第一存证消息，并基于所述信息系统标识生成第二存证消息；

或者，

接收所述第一存证消息，并基于信息系统标识，以及协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、信息系统的网络地址、信息系统的硬件地址、本地存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、第一存证消息完整性的度量值及签名、待生成的第二存证消息完整性的度量值及签名中的至少一种，生成第二存证消息；

将所述第二存证消息发送至所述中心存证系统，以使所述中心存证系统在接收到所述第二存证消息后生成第二存证收条；

在接收到所述中心存证系统返回的第二存证收条后，生成第一存证收条返回所述信息系统。

基于本地存证系统标识，生成第一存证收条返回所述信息系统；

或者，

基于本地存证系统标识，以及所述协议版本号、命令类别、存证事项类别、消息格式版本、数据包长度、自定义字段、第二存证收条标识、第二存证收条时间、第一存证收条标识、第一存证收条时间、信息系统标识、信息系统的网络地址、信息系统的硬件地址、中心存证系统的业务内部索引号、本地存证系统的业务内部索引号、信息系统的业务内部索引号、第一存证对象的类型、第一存证对象内容的标

题、第一存证对象的大小、第一存证对象内容的描述、第一存证对象内容的检索词、第一存证对象的分类号、第一存证对象的所属主体、第一存证对象的创建时间、第一存证对象的创建地点、第一存证对象的操作主体、第一存证对象的操作行为、第一存证对象的操作时间、第一存证对象的操作位置、第一存证对象的操作结果、第二存证对象的认证校验码、密文字段、第一存证消息完整性的度量值及签名、第二存证消息完整性的度量值及签名、第二存证收条完整性的度量值及签名和待生成的第一存证收条完整性的度量值及签名中的至少一种，生成第一存证收条返回所述信息系统。

图 8 示例了一种设备的实体结构示意图，如图 8 所示，该设备可以包括：处理器（processor）810、通信接口（Communications Interface）820、存储器（memory）830 和通信总线 840，其中，处理器 810，通信接口 820，存储器 830 通过通信总线 840 完成相互间的通信。处理器 810 可以调用存储器 830 中的逻辑指令，以执行存证方法，该方法包括：

确定第一存证对象，生成所述第一存证对象对应的存证请求，并将所述存证请求发送到存证系统；

接收所述存证系统返回的存证请求应答；

基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，并对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码；

基于所述认证校验码生成第一存证消息，并将所述第一存证消息发送到所述存证系统进行存证。

或者，处理器 810 可以调用存储器 830 中的逻辑指令，以执行存证方法，该方法包括：

接收信息系统发送的存证请求，所述存证请求与第一存证对象对应；

获取与所述存证请求对应的存证请求应答；

将所述存证请求应答返回到所述信息系统，以使所述信息系统基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码，并基于所述认证校验码生成第一存证消息；

基于所述信息系统发送的第一存证消息进行存证。

此外，上述的存储器 830 中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

另一方面，本发明还提供一种计算机程序产品，所述计算机程序产品包括计算机程序，计算机程序可存储在非暂态计算机可读存储介质上，所述计算机程序被处理器执行时，计算机能够执行上述各方法所提供的存证方法，该方法包括：

确定第一存证对象，生成所述第一存证对象对应的存证请求，并将所述存证请求发送到存证系统；

接收所述存证系统返回的存证请求应答；

基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，并对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码；

基于所述认证校验码生成第一存证消息，并将所述第一存证消息发送到所述存证系统进行存证。

或者，所述计算机程序被处理器执行时，计算机能够执行上述各方法所提供的存证方法，该方法包括：

接收信息系统发送的存证请求，所述存证请求与第一存证对象对应；

获取与所述存证请求对应的存证请求应答；

将所述存证请求应答返回到所述信息系统，以使所述信息系统基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码，并基于所述认证校验码生成第一存证消息；

基于所述信息系统发送的第一存证消息进行存证。

又一方面，本发明还提供一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现以执行上述各方法提供的存证方法，该方法包括：

确定第一存证对象，生成所述第一存证对象对应的存证请求，并将所述存证请求发送到存证系统；

接收所述存证系统返回的存证请求应答；

基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，并对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码；

基于所述认证校验码生成第一存证消息，并将所述第一存证消息发送到所述存证系统进行存证。

或者，该计算机程序被处理器执行时实现以执行上述各方法提供的存证方法，该方法包括：

接收信息系统发送的存证请求，所述存证请求与第一存证对象对

应；

获取与所述存证请求对应的存证请求应答；

将所述存证请求应答返回到所述信息系统，以使所述信息系统基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码，并基于所述认证校验码生成第一存证消息；

基于所述信息系统发送的第一存证消息进行存证。

以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行各个实施例或者实施例的某些部分所述的方法。

最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方

案的精神和范围。

说　明　书　附　图

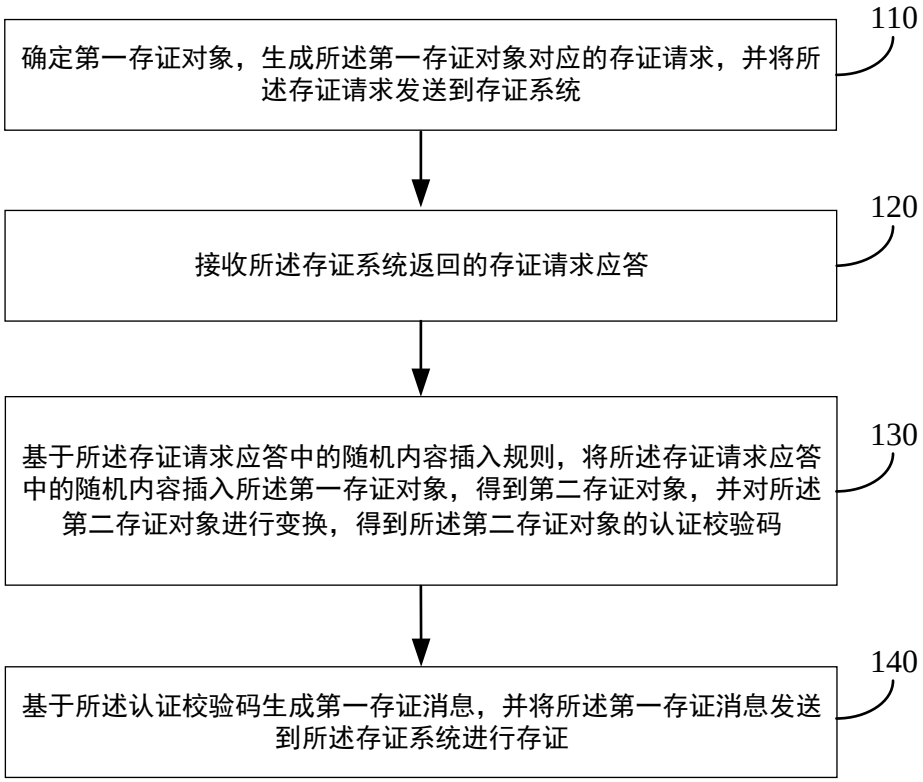

确定第一存证对象，生成所述第一存证对象对应的存证请求，并将所述存证请求发送到存证系统
110
接收所述存证系统返回的存证请求应答
120
基于所述存证请求应答中的随机内容插入规则，将所述存证请求应答中的随机内容插入所述第一存证对象，得到第二存证对象，并对所述第二存证对象进行变换，得到所述第二存证对象的认证校验码
130
基于所述认证校验码生成第一存证消息，并将所述第一存证消息发送到所述存证系统进行存证
140

图 1

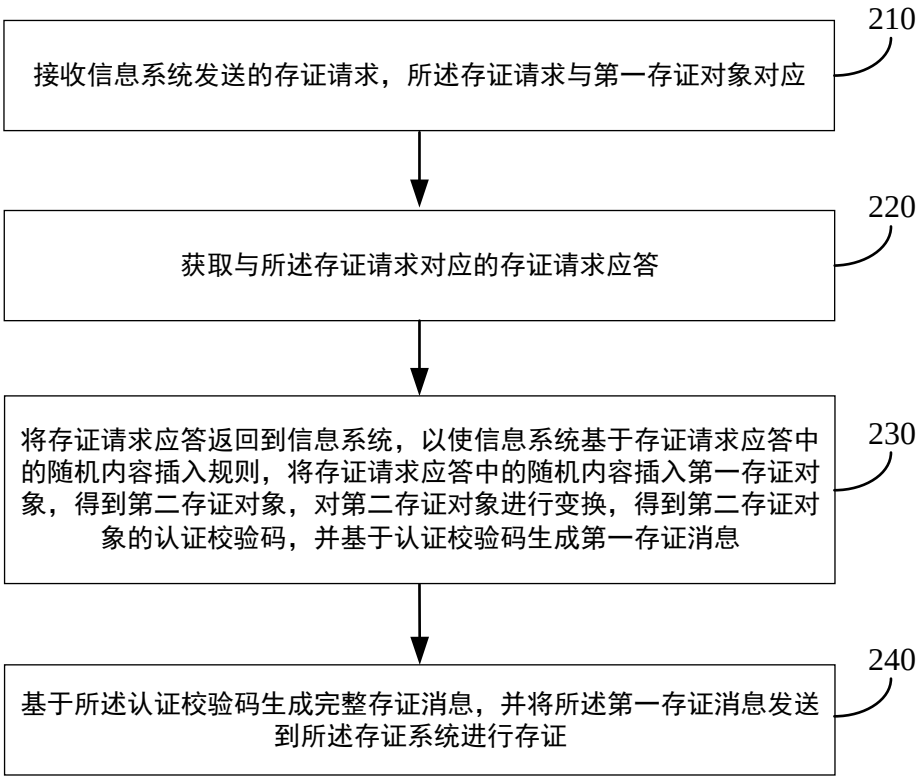

接收信息系统发送的存证请求，所述存证请求与第一存证对象对应
210
获取与所述存证请求对应的存证请求应答
220
将存证请求应答返回到信息系统，以使信息系统基于存证请求应答中的随机内容插入规则，将存证请求应答中的随机内容插入第一存证对象，得到第二存证对象，对第二存证对象进行变换，得到第二存证对象的认证校验码，并基于认证校验码生成第一存证消息
230
基于所述认证校验码生成完整存证消息，并将所述第一存证消息发送到所述存证系统进行存证
240

图 2

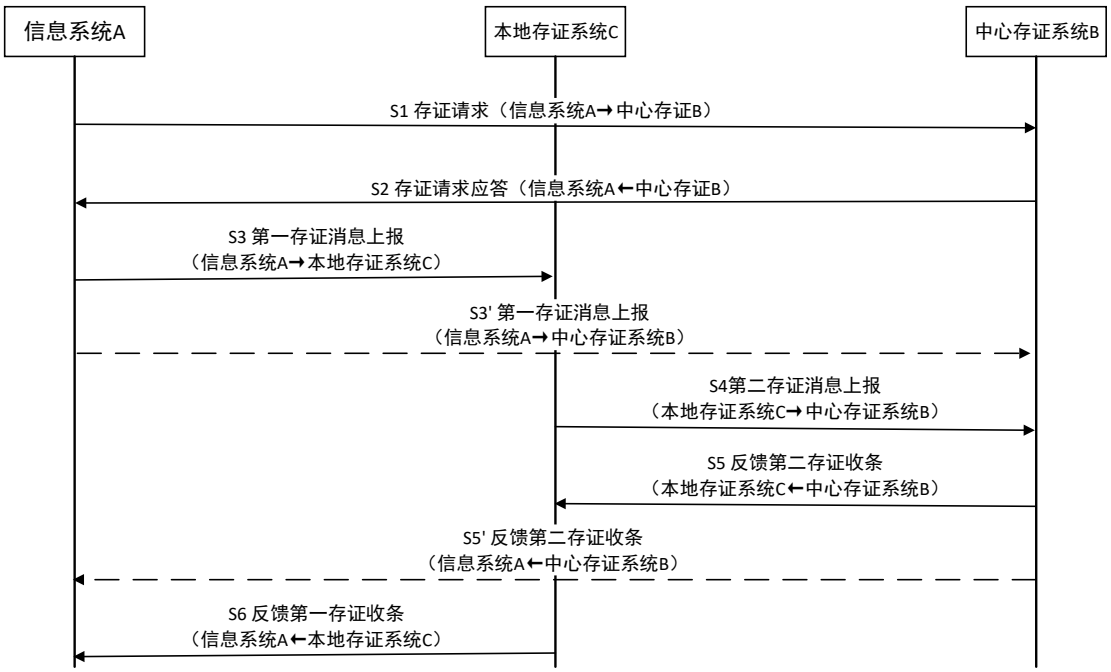

信息系统A
本地存证系统C
中心存证系统B
S1 存证请求（信息系统A→中心存证B）
S2 存证请求应答（信息系统A←中心存证B）
S3 第一存证消息上报
（信息系统A→本地存证系统C）
S3' 第一存证消息上报
（信息系统A→中心存证系统B）
S4第二存证消息上报
（本地存证系统C→中心存证系统B）
S5 反馈第二存证收条
（本地存证系统C←中心存证系统B）
S5' 反馈第二存证收条
（信息系统A←中心存证系统B）
S6 反馈第一存证收条
（信息系统A←本地存证系统C）

图 3

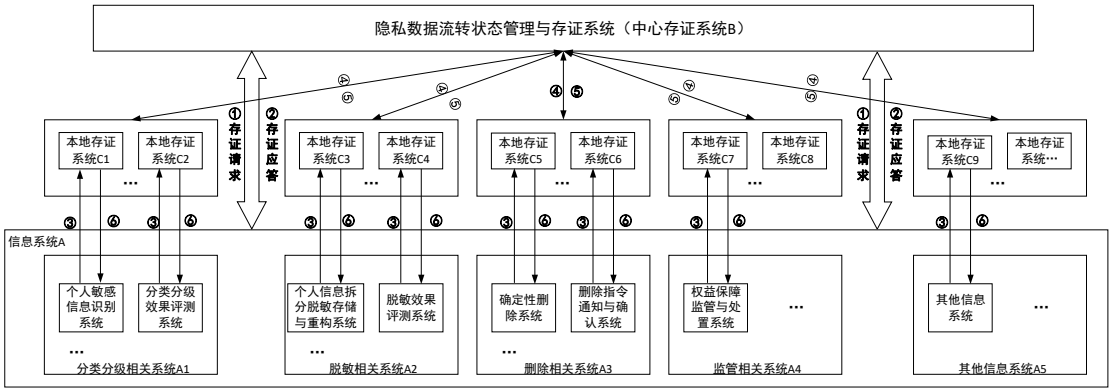

隐私数据流转状态管理与存证系统（中心存证系统B）
①存证请求
②存证应答
本地存证系统C1
本地存证系统C2
本地存证系统C3
本地存证系统C4
本地存证系统C5
本地存证系统C6
本地存证系统C7
本地存证系统C8
本地存证系统C9
本地存证系统…
信息系统A
个人敏感信息识别系统
分类分级效果评测系统
个人信息拆分脱敏存储与重构系统
脱敏效果评测系统
确定性删除系统
删除指令通知与确认系统
权益保障监管与处置系统
其他信息系统
分类分级相关系统A1
脱敏相关系统A2
删除相关系统A3
监管相关系统A4
其他信息系统A5

图 4

现有权利能不能保护此图，如果能保护不增加，说明书怎么描述请教程，中心任意一个和本地一个或多个连，本地一个信息系统，三方都是多对多

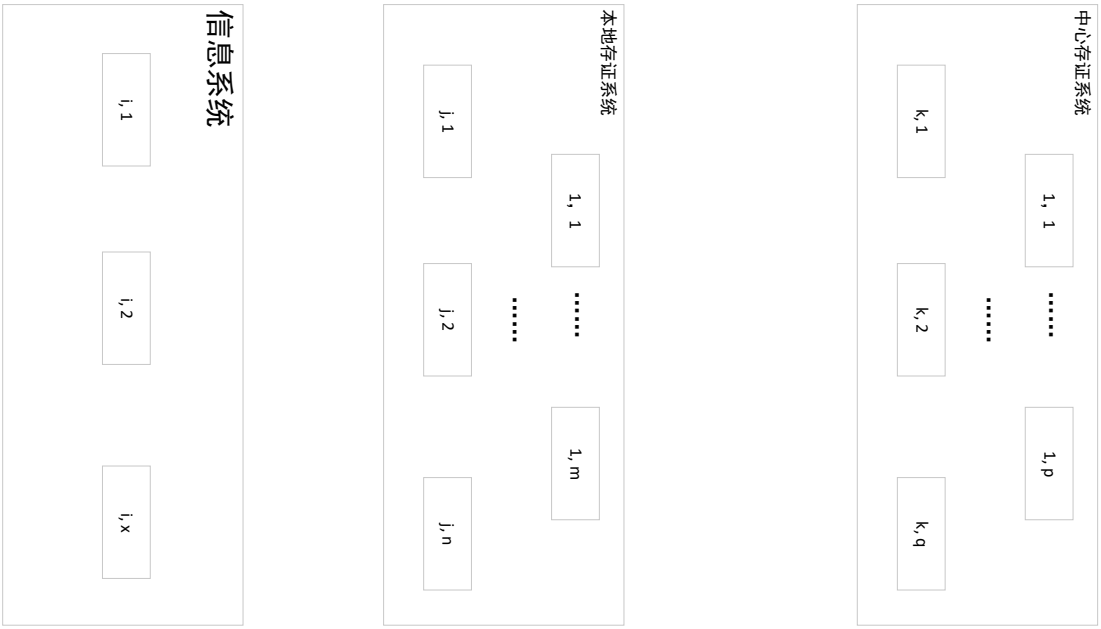


图 5

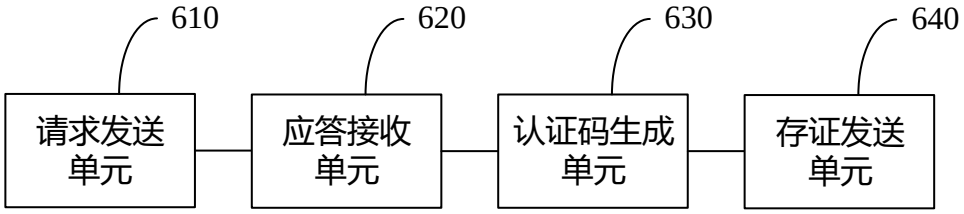


图 6

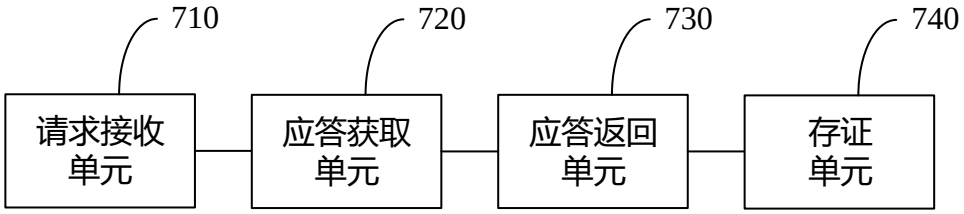


图 7

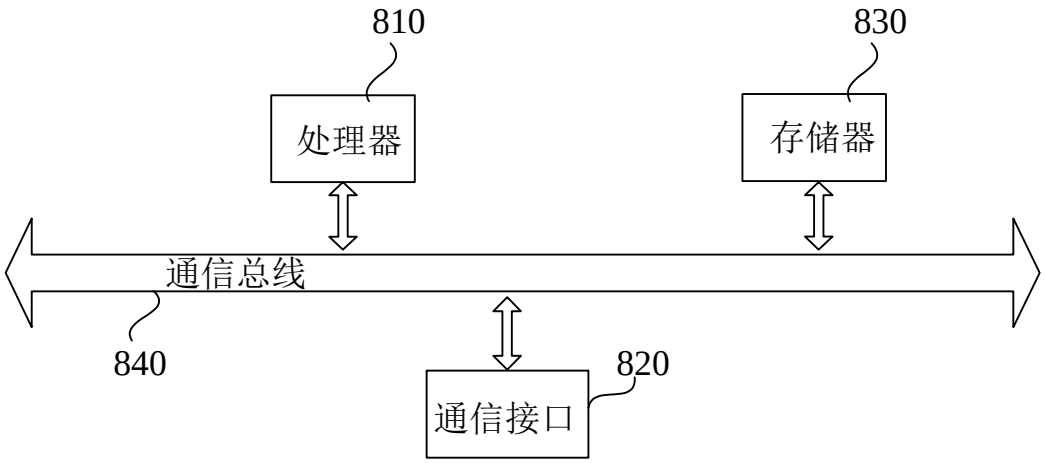


图 8