(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112217632 B
(45)授权公告日 2023.09.08

(21)申请号 202011085153.2

(22)申请日 2020.10.12

(65)同一申请的已公布的文献号
申请公布号 CN 112217632 A

(43)申请公布日 2021.01.12

(73)专利权人 国网数字科技控股有限公司
地址 100032 北京市西城区广义街7号楼8层8018室

(72)发明人 廖会敏 陈绍真 张程 周峰 王建文 陈平祥

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 储倩

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
G06F 21/46(2013.01)

(56)对比文件
CN 110059458 A,2019.07.26
CN 111464290 A,2020.07.28
CN 111638925 A,2020.09.08
CN 107493264 A,2017.12.19
CN 101447870 A,2009.06.03
CN 103368918 A,2013.10.23
CN 106341372 A,2017.01.18
US 2020067907 A1,2020.02.27
US 2016330028 A1,2016.11.10
WO 2012159191 A1,2012.11.29
CN 109981257 A,2019.07.05

审查员 刘星星

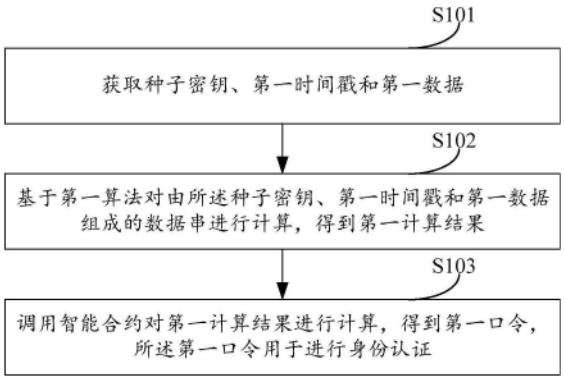
权利要求书1页 说明书5页 附图1页

(54)发明名称

一种基于智能合约和哈希链的身份认证方法及装置

(57)摘要

本申请实施例提供了一种基于智能合约和哈希链的身份认证方法，可以获取种子密钥、第一时间戳和第一数据，并基于第一算法对由所述种子密钥、第一时间戳和第一数据组成的数据串进行计算，得到第一计算结果。计算得到第一计算结果之后，不是如传统技术中那样，直接将第一计算结果作为口令，而是调用智能合约对第一计算结果继续进行计算，从而得到第一口令，第一口令用于进行身份认证。由此可见，即使第一算法、种子密钥、第一时间戳和第一数据均被破解，第一口令也无法被破解，若要破解第一口令，还需要破解前述智能合约。由此可见，利用本申请实施例的方案，可以降低第一口令被破解的可能性，从而降低安全风险。



CN 112217632 B

1.一种基于智能合约和哈希链的身份认证方法,其特征在于,所述方法包括:

获取种子密钥、第一时间戳和第一数据;

基于第一算法对由所述种子密钥、第一时间戳和第一数据组成的数据串进行计算,得到第一计算结果,所述第一计算结果包括N字节,N大于或者等于1;

调用智能合约对所述第一计算结果进行如下计算:

进行2*N次计算,其中:

在第1次计算时,首先利用算法k对所述第一计算结果进行计算,然后利用第一哈希算法对利用算法k对所述第一计算结果进行计算的计算结果进行哈希计算,其中:k的值根据所述第一计算结果的高4比特的值确定;

在第i次计算时,首先利用算法m对第(i-1)次计算的计算结果进行计算,然后利用所述第一哈希算法对利用算法m对所述(i-1)次计算的计算结果进行计算的计算结果进行哈希计算,其中:m的值根据所述第一计算结果的第(4*i-3)比特至所述第一计算结果的第4*i比特的值确定,i大于等于2,小于等于2*N;

将第2N次计算得到的计算结果,确定为第一口令。

2.根据权利要求1所述的方法,其特征在于,所述方法还包括:

接收第二口令;

比较所述第一口令和所述第二口令;

若所述第一口令等于所述第二口令,确定身份认证通过,若所述第一口令不等于所述第二口令,确定身份认证失败。

3.一种基于智能合约和哈希链的身份认证装置,其特征在于,所述装置包括:

获取单元,用于获取种子密钥、第一时间戳和第一数据;

第一计算单元,用于基于第一算法对由所述种子密钥、第一时间戳和第一数据组成的数据串进行计算,得到第一计算结果,所述第一计算结果包括N字节,N大于或者等于1;

第二计算单元,用于调用智能合约对所述第一计算结果进行如下计算:

进行2*N次计算,其中:

在第1次计算时,首先利用算法k对所述第一计算结果进行计算,然后利用第一哈希算法对利用算法k对所述第一计算结果进行计算的计算结果进行哈希计算,其中:k的值根据所述第一计算结果的高4比特的值确定;

在第i次计算时,首先利用算法m对第(i-1)次计算的计算结果进行计算,然后利用所述第一哈希算法对利用算法m对所述(i-1)次计算的计算结果进行计算的计算结果进行哈希计算,其中:m的值根据所述第一计算结果的第(4*i-3)比特至所述第一计算结果的第4*i比特的值确定,i大于等于2,小于等于2*N;

将第2N次计算得到的计算结果,确定为第一口令。

4.根据权利要求3所述的装置,其特征在于,所述装置还包括:

接收单元,用于接收第二口令;

比较单元,用于比较所述第一口令和所述第二口令;

认证单元,用于若所述第一口令等于所述第二口令,确定身份认证通过,若所述第一口令不等于所述第二口令,确定身份认证失败。

一种基于智能合约和哈希链的身份认证方法及装置

技术领域

[0001] 本申请涉及身份认证领域，特别是涉及一种基于智能合约和哈希链的身份认证方法及装置。

背景技术

[0002] 动态口令是一种常见的，成本较低、使用方便、安全可靠的一种身份认证方式。

[0003] 现有的动态口令生成方法为：利用某一算法对由种子密钥、时间戳、以及动态数据等组成的数据串进行计算，得到动态口令。

[0004] 但是，采用这种动态口令生成方式，动态口令被破解的可能性比较高，从而带来一定的安全风险。

发明内容

[0005] 本申请所要解决的技术问题是现有技术中动态口令被破解的可能性比较高，从而带来一定的安全风险，提供一种基于智能合约和哈希链的身份认证方法及装置。

[0006] 第一方面，本申请实施例提供了一种基于智能合约和哈希链的身份认证方法，所述方法包括：

[0007] 获取种子密钥、第一时间戳和第一数据；

[0008] 基于第一算法对由所述种子密钥、第一时间戳和第一数据组成的数据串进行计算，得到第一计算结果，所述第一计算结果包括N字节，N大于或者等于1；

[0009] 调用智能合约对所述第一计算结果进行如下计算：

[0010] 进行2*N次计算，其中：

[0011] 在第1次计算时，基于算法k和第一哈希算法对所述第一计算结果进行计算，其中：k的值根据所述第一计算结果的高4比特的值确定；

[0012] 在第i次计算时，基于算法m和所述第一哈希算法对第(i-1)次计算的计算结果进行计算，其中：k的值根据所述第一计算结果的第(4*i-3)比特至所述第一计算结果的第4*i比特的值确定，i大于等于2，小于等于2*N；

[0013] 将第2N次计算得到的计算结果，确定为所述第一口令。

[0014] 在一种实现方式中，所述方法还包括：

[0015] 接收第二口令；

[0016] 比较所述第一口令和所述第二口令；

[0017] 若所述第一口令等于所述第二口令，确定身份认证通过，若所述第一口令不等于所述第二口令，确定身份认证失败。

[0018] 第二方面，本申请实施例提供了一种基于智能合约和哈希链的身份认证装置，所述装置包括：

[0019] 获取单元，用于获取种子密钥、第一时间戳和第一数据；

[0020] 第一计算单元，用于基于第一算法对由所述种子密钥、第一时间戳和第一数据组

成的数据串进行计算，得到第一计算结果，所述第一计算结果包括N字节，N大于或者等于1；

[0021] 第二计算单元，用于调用智能合约对所述第一计算结果进行如下计算：

[0022] 进行2*N次计算，其中：

[0023] 在第1次计算时，基于算法k和第一哈希算法对所述第一计算结果进行计算，其中：k的值根据所述第一计算结果的高4比特的值确定；

[0024] 在第i次计算时，基于算法m和所述第一哈希算法对第(i-1)次计算的计算结果进行计算，其中：k的值根据所述第一计算结果的第(4*i-3)比特至所述第一计算结果的第4*i比特的值确定，i大于等于2，小于等于2*N；

[0025] 将第2N次计算得到的计算结果，确定为所述第一口令。

[0026] 在一种实现方式中，所述装置还包括：

[0027] 接收单元，用于接收第二口令；

[0028] 比较单元，用于比较所述第一口令和所述第二口令；

[0029] 认证单元，用于若所述第一口令等于所述第二口令，确定身份认证通过，若所述第一口令不等于所述第二口令，确定身份认证失败。

[0030] 与现有技术相比，本申请实施例具有以下优点：

[0031] 本申请实施例提供了一种基于智能合约和哈希链的身份认证方法，具体地，可以获取种子密钥、第一时间戳和第一数据，并基于第一算法对由所述种子密钥、第一时间戳和第一数据组成的数据串进行计算，得到第一计算结果。计算得到第一计算结果之后，不是如传统技术中那样，直接将第一计算结果作为口令，而是调用智能合约对第一计算结果继续进行计算，从而得到第一口令，第一口令用于进行身份认证。由此可见，利用本申请实施例的方案，即使第一算法、种子密钥、第一时间戳和第一数据均被破解，第一口令也无法被破解，因为第一口令是基于调用智能合约对所述第一计算结果进行计算得到的。若要破解第一口令，还需要破解前述智能合约。由此可见，利用本申请实施例的方案，可以降低第一口令被破解的可能性，从而降低安全风险。

附图说明

[0032] 为了更清楚地说明本申请实施例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简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施例，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。

[0033] 图1为本申请实施例提供的一种基于智能合约和哈希链的身份认证方法的流程示意图；

[0034] 图2为本申请实施例提供的一种基于智能合约和哈希链的身份认证装置的结构示意图。

具体实施方式

[0035] 为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在

没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0036] 本申请的发明人经过研究发现，动态口令生成方法为：利用某一算法对由种子密钥、时间戳、以及动态数据等组成的数据串进行计算，得到动态口令。其中，动态令牌和服务器均可以采用上述方法生成动态口令。动态令牌指的是为用户生成动态口令的设备。

[0037] 在一个示例中，动态令牌可以通过上述方式生成动态口令1，用户可以通过动态令牌获取动态口令1，然后通过终端设备将该动态口令1发送给服务器。例如，用户在终端设备的应用程序上输入该动态口令1，从而使得终端设备将该动态口令1发送给服务器。服务器可以通过上述方式生成动态口令2，并比较动态口令1和动态口令2，从而实现身份认证。

[0038] 但是，采用这种动态口令生成方式，动态口令被破解的可能性比较高。因为一旦前述“某一算法”、种子密钥、时间戳、以及动态数据被破解，则生成的动态口令(例如动态口令1和动态口令2)即可被破解。而动态口令一旦被破解，就会导致身份认证的结果不可信，从而带来一定的安全隐患。

[0039] 为了解决上述问题，本申请实施例提供了一种基于智能合约和哈希链的身份认证方法，可以降低第一口令被破解的可能性，从而降低安全风险。

[0040] 下面结合附图，详细说明本申请的各种非限制性实施方式。

[0041] 示例性方法

[0042] 参见图1，该图为本申请实施例提供的一种基于智能合约和哈希链的身份认证方法的流程示意图。

[0043] 图1所示的方法，可以由动态令牌执行，也可以由服务器执行，本申请实施例不做具体限定。

[0044] 图1所述的方法，可以包括如下S101-S103。

[0045] S101：获取种子密钥、第一时间戳和第一数据。

[0046] S102：基于第一算法对由所述种子密钥、第一时间戳和第一数据组成的数据串进行计算，得到第一计算结果。

[0047] 关于S101和S102需要说明的是，其与传统的动态口令生成方式类似，故此处不做详细说明。

[0048] S103：调用智能合约对第一计算结果进行计算，得到第一口令，所述第一口令用于进行身份认证。

[0049] 计算得到第一计算结果之后，不是如传统技术中那样，直接将第一计算结果作为口令，而是调用智能合约再次对所述第一计算结果进行计算，得到第一口令，第一口令用于进行身份认证。其中，第一口令可以是基于智能合约再次对所述第一计算结果进行计算得到的计算结果，也可以是基于智能合约再次对所述第一计算结果进行计算得到的计算结果的一部分，例如是基于至少一个算法再次对所述第一计算结果进行计算得到的计算结果的前6位。

[0050] 由此可见，利用本申请实施例的方案，即使第一算法、种子密钥、第一时间戳和第一数据均被破解，第一口令也无法被破解，因为第一口令是基于智能合约对所述第一计算结果进行计算得到的。若要破解第一口令，还需要破解智能合约。由此可见，利用本申请实施例的方案，可以降低第一口令被破解的可能性，从而降低安全风险。

[0051] 在一个示例中，所述第一计算结果包括N字节，S103在具体实现时，可以基于所述

第一计算结果进行2*N次计算。例如，第一计算结果为0x35E8，则第一计算结果包括2字节，故需要进行4次计算。其中，一次计算利用一种算法。具体地：

[0052] 在第1次计算时，基于算法k和第一哈希算法对所述第一计算结果进行计算，其中：k的值根据所述第一计算结果的高4比特的值确定。例如，第一计算结果为0x35E8，高4比特的值为3，则在第1次计算时，利用算法3和第一哈希算法对第一计算结果进行计算。例如，首先利用算法3对第一计算结果进行计算，然后利用第一哈希算法对利用算法3对第一计算结果进行计算的计算结果进行哈希计算。

[0053] 在第i次计算时，基于算法m和第一哈希算法对第(i-1)次计算的计算结果进行计算，其中:k的值根据所述第一计算结果的第(4*i-3)比特至所述第一计算结果的第4*i比特的值确定，i大于等于2，小于等于2*N。第2*N次计算之后，可以将第2*N次计算得到的计算结果，确定为所述第一口令。

[0054] 以第一计算结果为0x35E8举例说明:第2次计算时，采用算法5和第一哈希算法对第一次计算的计算结果进行计算;第3次计算时，采用算法14(16进制E对应10进制数14)和第一哈希算法对第二次计算的计算结果进行计算;第4次计算时，采用算法8和第一哈希算法对第三次计算的计算结果进行计算。第4次计算得到的计算结果即为第一口令。

[0055] 其中，对于算法3、算法5、算法14和算法8所采用的具体算法，本申请实施例不做具体限定。在一个示例中，可以预先确定16种算法，分别从算法1、算法2至算法16，而后，根据(4*i-3)比特至所述第一计算结果的第4*i比特的值，从该16种算法中确定第i次计算所采用的算法。其中，这16种算法可以是不同的哈希算法。

[0056] 可以理解的是，由于在进行2*N次计算时，每次计算所使用的算法根据第一计算结果的值确定，而不是每次进行动态口令的计算时，都采用相同的计算方式，因此，采用这种方式，为第一口令的计算方式增加了一定的随机性，从而增加了破解计算得到的动态口令(例如第一口令)的难度，从而进一步提升了安全性。

[0057] 若以上图1所示的方法由动态令牌执行，则用户可以通过终端设备将该第一口令发送给服务器，例如，用户在终端设备的应用程序上输入该第一口令，从而使得终端设备将该第一口令发送给服务器。服务器接收到第一口令之后，可以基于图1所示的方法生成第二口令，并比较第一口令和第二口令，从而完成身份认证。具体地，若所述第一口令等于所述第二口令，确定身份认证通过，若所述第一口令不等于所述第二口令，确定身份认证失败。

[0058] 若以上图1所示的方法由服务器执行，则服务器还可以接收来自于终端设备的第二口令，并比较第一口令和第二口令，从而完成身份认证。具体地，若所述第一口令等于所述第二口令，确定身份认证通过，若所述第一口令不等于所述第二口令，确定身份认证失败。其中，第二口令可以是动态令牌生成，并由用户通过终端设备发送给服务器的，动态令牌生成第二口令的方式可以参考以上图1所示的方法，此处不再详述。

[0059] 示例性设备

[0060] 基于以上实施例提供的方法，本申请实施例还提供了一种装置，以下结合附图介绍该装置。

[0061] 参见图2，该图为本申请实施例提供的一种基于智能合约和哈希链的身份认证装置的结构示意图。所述装置200例如可以具体包括:获取单元201、第一计算单元202和第二计算单元203。

[0062] 获取单元201,用于获取种子密钥、第一时间戳和第一数据;

[0063] 第一计算单元202,用于基于第一算法对由所述种子密钥、第一时间戳和第一数据组成的数据串进行计算,得到第一计算结果,所述第一计算结果包括N字节,N大于或者等于1;

[0064] 第二计算单元203,用于调用智能合约对所述第一计算结果进行如下计算:

[0065] 进行2*N次计算,其中:

[0066] 在第1次计算时,基于算法k和第一哈希算法对所述第一计算结果进行计算,其中:k的值根据所述第一计算结果的高4比特的值确定;

[0067] 在第i次计算时,基于算法m和所述第一哈希算法对第(i-1)次计算的计算结果进行计算,其中:k的值根据所述第一计算结果的第(4*i-3)比特至所述第一计算结果的第4*i比特的值确定,i大于等于2,小于等于2*N;

[0068] 将第2N次计算得到的计算结果,确定为所述第一口令。

[0069] 在一种实现方式中,所述装置200还包括:

[0070] 接收单元,用于接收第二口令;

[0071] 比较单元,用于比较所述第一口令和所述第二口令;

[0072] 认证单元,用于若所述第一口令等于所述第二口令,确定身份认证通过,若所述第一口令不等于所述第二口令,确定身份认证失败。

[0073] 由于所述装置200是与以上方法实施例提供的方法对应的装置,所述装置200的各个单元的具体实现,均与以上方法实施例为同一构思,因此,关于所述装置200的各个单元的具体实现,可以参考以上方法实施例的描述部分,此处不再赘述。

[0074] 本领域技术人员在考虑说明书及实践这里公开的发明后,将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化,这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的,本申请的真正范围和精神由下面的权利要求指出。

[0075] 应当理解的是,本申请并不局限于上面已经描述并在附图中示出的精确结构,并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制

[0076] 以上所述仅为本申请的较佳实施例,并不用以限制本申请,凡在本申请的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本申请的保护范围之内。

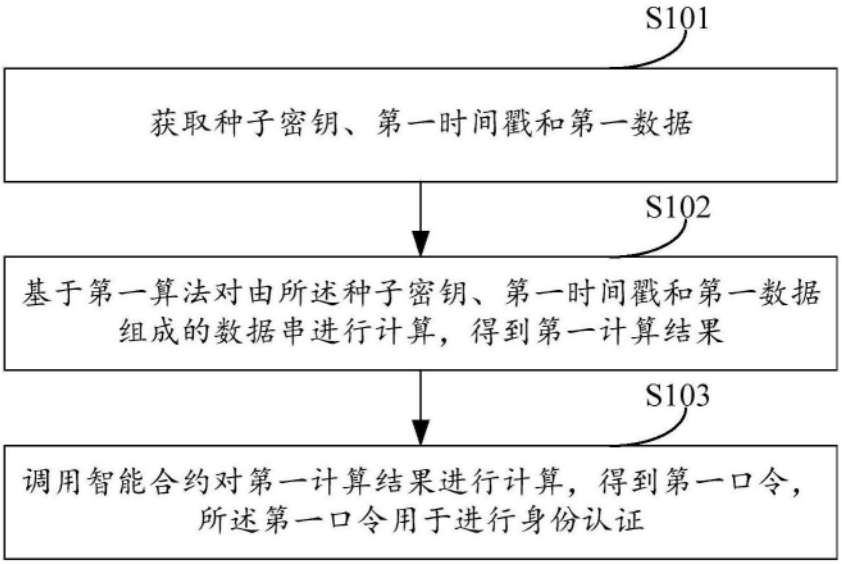

S101
获取种子密钥、第一时间戳和第一数据
S102
基于第一算法对由所述种子密钥、第一时间戳和第一数据组成的数据串进行计算，得到第一计算结果
S103
调用智能合约对第一计算结果进行计算，得到第一口令，所述第一口令用于进行身份认证

图1

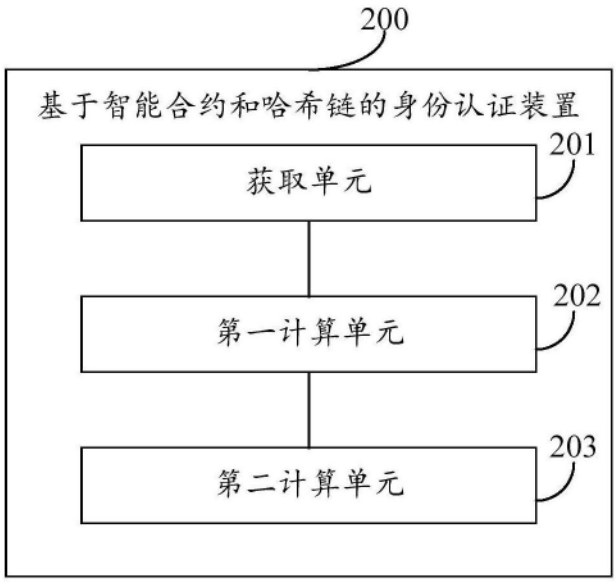

200
基于智能合约和哈希链的身份认证装置
201
获取单元
202
第一计算单元
203
第二计算单元

图2