(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101345623 B
(45)授权公告日 2010.11.10

(21)申请号 200710128162.3

(22)申请日 2007.07.09

(73)专利权人 中茂电子(深圳)有限公司
地址 518054 广东省深圳市南山区登良路天安南油工业区4栋第八层

(72)发明人 陈泓斌 曾焕舜

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 任默闻

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/16(2006.01)

(56)对比文件
CN 1695340 A,2005.11.09, 说明书第6页第10段-第9页第7段、图1-4.
US 2007/0081667 A1,2007.04.12, 全文.
CN 1695340 A,2005.11.09, 说明书第6页第10段-第9页第7段、图1-4.
CN 1559117 A,2004.12.29, 全文.
CN 1527208 A,2004.09.08, 说明书第2页倒数第6段,第2页倒数第1段-第3页第1段.
CN 1558584 A,2004.12.29, 全文.

审查员 杨盈霄

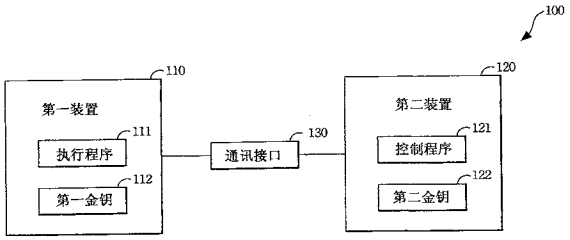
权利要求书 1 页 说明书 4 页 附图 3 页

(54)发明名称

具有认证功能的控制系统及方法

(57)摘要

一种具有认证功能的控制系统,目的是保护发明人所开发的程序以及设备,该控制系统包括一第一装置以及一第二装置;第一装置包括一执行程序以及一第一金钥,第一金钥具有信息加密与解密的功能,执行程序用以控制第一装置,第二装置透过一通讯接口与第一装置相连接;第二装置包含一控制程序以及一第二金钥,第二金钥具有信息加密与解密的功能,此外,第一金钥的加密信息必须利用第二金钥解密,且第二金钥的加密信息必须利用第一金钥解密,第一金钥以及第二金钥需同时搭配以符合认证,第一装置以及第二装置才能执行功能。



CN 101345623 B

1. 一种具有认证功能的控制系统，包括：

一第一装置，包含一执行程序以及一第一金钥，所述的第一金钥具有信息加密与解密的功能，所述第一金钥分为一部分固定金钥以及一部分动态金钥，所述的部分动态金钥由所述的第一装置随机产生；以及

一第二装置，与所述的第一装置连结，其包括一控制程序以及一第二金钥，所述的第二金钥具有信息加密与解密的功能，所述第二金钥分为一部分固定金钥以及一部分动态金钥；

其中，所述的第一金钥的加密信息必须利用所述的第二金钥解密，且所述的第二金钥的加密信息必须利用所述的第一金钥解密，而所述的控制程序可控制所述的执行程序，第一金钥的动态金钥在执行阶段加密后传递给第二装置，第二装置接收该加密后的第一金钥动态金钥，译码后与第二金钥的固定金钥组成完整的第二金钥。

2. 如权利要求 1 所述的控制系统，其特征在于，所述的第一装置与所述的第二装置以一通讯接口作为连结，所述的通讯接口包括 GPIB、RS232、RS482、RS485、USB、Ethernet 或上述的组合。

3. 如权利要求 1 所述的控制系统，其特征在于，所述的加密和解密技术的算法包括 DES、Triple-DES、AES、RC5、RC6 或上述的组合。

4. 一种控制系统的认证方法，所述的控制系统包括一第一装置具有一第一金钥，所述第一金钥分为一部分固定金钥以及一部分动态金钥，以及一第二装置具有一第二金钥，所述第二金钥分为一部分固定金钥以及一部分动态金钥，其中，第一金钥的动态金钥在执行阶段加密后传递给第二装置，第二装置接收该加密后的第一金钥动态金钥，译码后与第二金钥的固定金钥组成完整的第二金钥，所述的认证方法包括：

a. 所述的第一装置随机产生一第一信息，并利用所述的第一金钥对所述的第一信息进行加密以产生第一加密信息；

b. 所述的第一装置将所述的第一加密信息传送至所述的第二装置；

c. 所述的第二装置利用所述的第二金钥将所述的第一加密信息解密，并获得一第二信息；

d. 所述的第二装置将所述的第二信息回传至所述的第一装置；

e. 所述的第一装置判断所述的第二信息是否与所述的第一信息相同，若为是则所述的第二装置取得所述的第一装置的控制权限。

5. 如权利要求 4 所述的认证方法，其特征在于，所述的第 (a) 步骤可为所述的第一装置随机产生一第一信息，并利用所述的第一金钥对所述的第一信息以及部分第一金钥内容进行加密以产生第一加密信息。

6. 如权利要求 4 所述的认证方法，其特征在于，所述的第一装置与所述的第二装置以一通讯接口作为连结，所述的通讯接口包括 GPIB、RS232、RS482、RS485、USB、Ethernet 或上述的组合。

7. 如权利要求 4 所述的认证方法，其特征在于，所述的加密和解密技术的算法包括 DES、Triple-DES、AES、RC5、RC6 或上述的组合。

具有认证功能的控制系统及方法

技术领域

[0001] 本发明关于一种认证装置及其相关的方法，特别是指一种可使该认证装置以及方法达到保护发明人所开发的程序以及设备的功效，具体来说是关于一种具有认证功能的控制系统及方法。

背景技术

[0002] 目前一般常见的可远程控制的仪器，控制的命令在标准的通讯接口上都是公开的，有心人士只要设计相同的命令格式，即可使用现成的软件，造成开发软件仪器商的损失；部分仪器厂商会使用特殊的通讯接口来避免被抄袭，但开发新的通讯接口，也将提高开发的成本及维护的困难。而在软件部份，一般常见的保护方式如注册码、软件启动等，都无法有效的防止破解，而使用硬件锁为另一个选择，但同样也会增加产品的成本，也由于市面上有一定加密强度的硬件锁不多，自然成为所有黑客的攻击目标，其厂商也需公开其开发的方式给软件厂商，造成只要破解一个硬件锁，所有使用此产品的软件保护全部瓦解。

[0003] 一般现有技术如台湾专利公告第 480435 号的“IC 智能卡安全系统”，其中包含：

[0004] 一安装于计算机内，用于储存辨识数据 (authenticating data) 的互补金属氧半导体存储器 (CMOS memory)；

[0005] 一用于储存备份密码的备份媒体；以及

[0006] 一种装置，用于处理 (processing) 上述互补金属氧半导体存储器中的上述辨识数据，上述 IC 智能卡中的上述密码，以及上述备份媒体中的上述备份密码；其中计算机于确认备份密码与辨识数据一致后得以启动。

[0007] 虽然上述的现有技术可达到加密以及解密的功能，但是由于其加、解密程序为固定的模式并无法随机改变，且于该系统中需先以辨识数据于各类装置中辨识出其所属的装置，再利用备份密码进行确认动作，加、解密时仅具有单向保护机制，又该设定的密码无法作动态的改变；故以一般的现有技术并无法符合使用者的所需。

发明内容

[0008] 本发明鉴于上述现有技术的缺失，开发出一套认证装置以及方法，可通过该装置以及方法可确保使用者于使用本发明所开发的程序时，必须同时搭配本发明所开发的设备，为确实保护发明人的权益，乃提出本发明，通过本发明的提出，改善现行技术的缺失，以对相关设计制造业者有所裨益。

[0009] 本发明的目的在于提供一种认证装置及其相关的方法，用于使该认证装置以及方法达到保护发明人所开发的程序以及设备的功效。

[0010] 本发明具有认证功能的控制系统包括一第一装置以及一第二装置。

[0011] 第一装置包括一执行程序以及一第一金钥，第一金钥具有信息加密与解密的功能，执行程序用以控制该第一装置，第二装置透过一通讯接口与第一装置相连接；第二装置包含一控制程序以及一第二金钥，第二金钥具有信息加密与解密的功能。此外，第一金钥的

加密信息必须利用第二金钥解密，且第二金钥的加密信息必须利用第一金钥解密，而控制程序可控制执行程序，执行程序系用以控制第一装置，第一金钥以及第二金钥需同时搭配以符合认证，第一装置以及第二装置才能执行功能。

[0012] 本发明的设计属于对称金钥加密法，由于其加、解密程序系随机改变的，且第一装置与第二装置直接相连接的，可直接利用本身的金钥直接进行确认他方信息的动作，第二金钥可对第一装置所加密的信息进行解密，再回传给第一装置作比对，故可达到双向保护机制的功效。

[0013] 其步骤由第一装置随机产生一第一信息，并利用第一金钥进行加密以产生第一加密信息，再将该第一加密信息传送至第二装置，第二装置利用第二金钥将第一加密信息解密，并获得一第二信息，第二装置将第二信息回传至第一装置，第一装置判断第二信息是否与第一信息相同，若比对结果不相同，则回到最初步骤，代表该第二装置不具第二金钥，非合格的装置无法演算出正确的信息，若比对结果相同则认证完成，代表双方皆为合格装置，第二装置取得第一装置的控制权限。

[0014] 由于每次第一装置以及第二装置送出的信息系随机的，也有可能是假的，因此在通讯接口的信道上，拦截下来的信息每次都不相同，无法经由信息归纳求出内容，而第一金钥以及第二金钥在最后执行阶段才组合，所以无法由破解软件取得正确金钥内容，所以透过这样的机制，可使该具有认证功能的控制系统达到双向保护机制，且加密、解密程序随机加入乱码，严格把关使其不受有心人士破解，本发明可以确保使用者在使用本发明所开发的程序以及设备时，必须要包含一定机种、一定数量的我方仪器，当然，该具有认证功能的控制系统仍保有可任意扩充其它硬件的弹性。

[0015] 是以，通过上述本发明所揭示的具有认证功能的控制系统及方法的说明实例，本发明所开发的程序以及设备的确实可达到受保护的功效。

附图说明

[0016] 图 1 :本发明的认证功能的控制系统的示意图。

[0017] 图 2 :本发明控制系统的认证方法的第一实施例流程图。

[0018] 图 3 :本发明控制系统的认证方法的第二实施例流程图。

[0019] 附图标号 :

[0020] 100 :控制系统

[0021] 110 :第一装置

[0022] 111 :执行程序

[0023] 112 :第一金钥

[0024] 120 :第二装置

[0025] 121 :控制程序

[0026] 122 :第二金钥

[0027] 130 :通讯接口

[0028] S1 ～ S6 :各个步骤流程

[0029] S1’～ S6’:各个步骤流程

具体实施方式

[0030] 关于本发明所述的具有认证功能的控制系统及方法，可以通过以下发明详述及所附图式，得到进一步的了解。

[0031] 由于目前仪器的通讯接口有非常多的种类，如GPIB、RS232/482/485、USB、Ethernet等，因此本发明将以适用于所有的机种，这些常见的通讯接口用于信息传输时，其内容是可被监控的，意指这些通讯数据是完全公开的，所以本发明设计出一种认证装置及其相关的方法，即使通讯数据完全公开，也能达到保密的效果，以下将详细叙述本发明的设计。

[0032] 首先，请先参阅图1，其为本发明设计的基本概念，亦为本发明具有认证功能的控制系统的示意图，该控制系统100包括一第一装置110以及一第二装置120。

[0033] 其中，第一装置110包括一执行程序111以及一第一金钥112，第一金钥112具有信息加密与解密的功能，第一装置110的执行程序111系用以控制该第一装置110，第二装置120可为一系统主控端、一个人计算机(PC)、一个人数字助理(PDA)、一电子书包或一电玩设备等，透过一通讯接口130与该第一装置110相连接，通讯接口130包括GPIB、RS232、RS482、RS485、USB、Ethernet或上述的组合；第二装置120包含一控制程序121以及一第二金钥122，第二金钥122具有信息加密与解密的功能，以上的加密、解密技术的算法包括DES、Triple-DES、AES、RC5、RC6或上述的组合；第一金钥112以及第二金钥122的加密信息可为一认证码或一随机随机数。此外，第一金钥112的加密信息必须利用第二金钥122解密，且第二金钥122的加密信息必须利用第一金钥112解密，而控制程序121可控制执行程序112，执行程序112用以控制第一装置110，第一金钥112以及第二金钥122需同时搭配以符合认证，第一装置110以及第二装置120才能执行功能。

[0034] 本发明的设计属于对称金钥加密法，由于其加、解密程序是随机改变的，且第一装置110是与第二装置120直接相连接的，可直接利用本身的金钥直接进行确认他方信息的动作，第二金钥122可对第一装置110所加密的信息进行解密，再回传给第一装置110作比对，故可达到双向保护机制的功效。

[0035] 请先参阅图2，其为本发明控制系统的认证方法的第一实施例流程图，第一装置随机产生一第一信息，并利用第一金钥进行加密以产生第一加密信息（步骤S 1），再将该第一加密信息传送至第二装置（步骤S2），第二装置利用第二金钥将第一加密信息解密，并获得一第二信息（步骤S3），第二装置将第二信息回传至第一装置（步骤S4），第一装置判断第二信息是否与第一信息相同（步骤S5），若比对结果不相同，则回到步骤S1，代表该第二装置不具第二金钥，非合格的装置无法演算出正确的信息，若比对结果相同则认证完成，代表双方皆为合格装置，第二装置取得第一装置的控制权限（步骤S6）。

[0036] 请先参阅图3，其为本发明控制系统的认证方法的第二实施例流程图，其步骤与第一实施例相似，不同的处在于，第一装置与第二装置的功能对调，第二装置随机产生一第一信息，并利用第二金钥进行加密以产生第一加密信息（步骤S1’），再将该第一加密信息传送至第一装置（步骤S2’），第一装置利用第一金钥将第一加密信息解密，并获得一第二信息（步骤S3’），第一装置将第二信息回传至第二装置（步骤S4’），第二装置判断第二信息是否与第一信息相同（步骤S5’），若比对结果不相同，则回到步骤S1’，代表该第一装置不具第一金钥，非合格的装置无法演算出正确的信息，若比对结果相同则认证完成，代表双方

皆为合格装置，第一装置取得第二装置的控制权限（步骤 S6’）。

[0037] 第一金钥 112 可分为一部份固定金钥，一部分动态金钥，第二金钥 122 亦分为一部分固定金钥、一部份动态金钥，动态金钥系随机产生的，每一次产生的内容皆不相同，第一金钥 112 的动态金钥在执行阶段透过特殊编码加密后传递给第二装置 120，第二装置 120 接收此部份编码加密后的第一金钥 112 动态金钥，译码后与其它部份第二金钥的固定金钥组成完整第二金钥 122，此时第二金钥 122 与第一金钥 112 系相同的，但第一金钥 112 的某一部份是透过动态产生再编码传递，可以让金钥每次皆不同，以避免有心人士破解。

[0038] 由于每次第一装置 110 以及第二装置 120 送出的信息是随机的，也有可能是假的，因此在通讯接口的信道上，拦截下来的信息每次都不相同，无法经由信息归纳求出内容，而第一金钥 112 以及第二金钥 122 在最后执行阶段才组合，所以无法由破解软件取得正确金钥内容，所以透过这样的机制，可使该具有认证功能的控制系统 100 达到双向保护机制，且加密、解密程序随机加入乱码，严格把关使其不受有心人士破解，本发明可以确保使用者在使用本发明人所开发的程序以及设备时，必须要包含一定机种的我方仪器，意指具有第二金钥 122 的第二装置 120 为必要装置，且必须要包含有一定数量的我方仪器，意指第二金钥 122 可分为复数个部分金钥设于第二装置 120 中，当然，该具有认证功能的控制系统仍保有可任意扩充其它硬件的弹性。

[0039] 是以，通过上述本发明所揭示的具有认证功能的控制系统及方法的说明实例，发明人所开发的程序以及设备的确实可达到受保护的功效。

[0040] 本发明虽以较佳实例阐明如上，然其并非用以限定本发明的精神与发明实体仅止于上述实施例。是以，在不脱离本发明的精神与范围内所作的修改，均应包括在权利要求范围内。

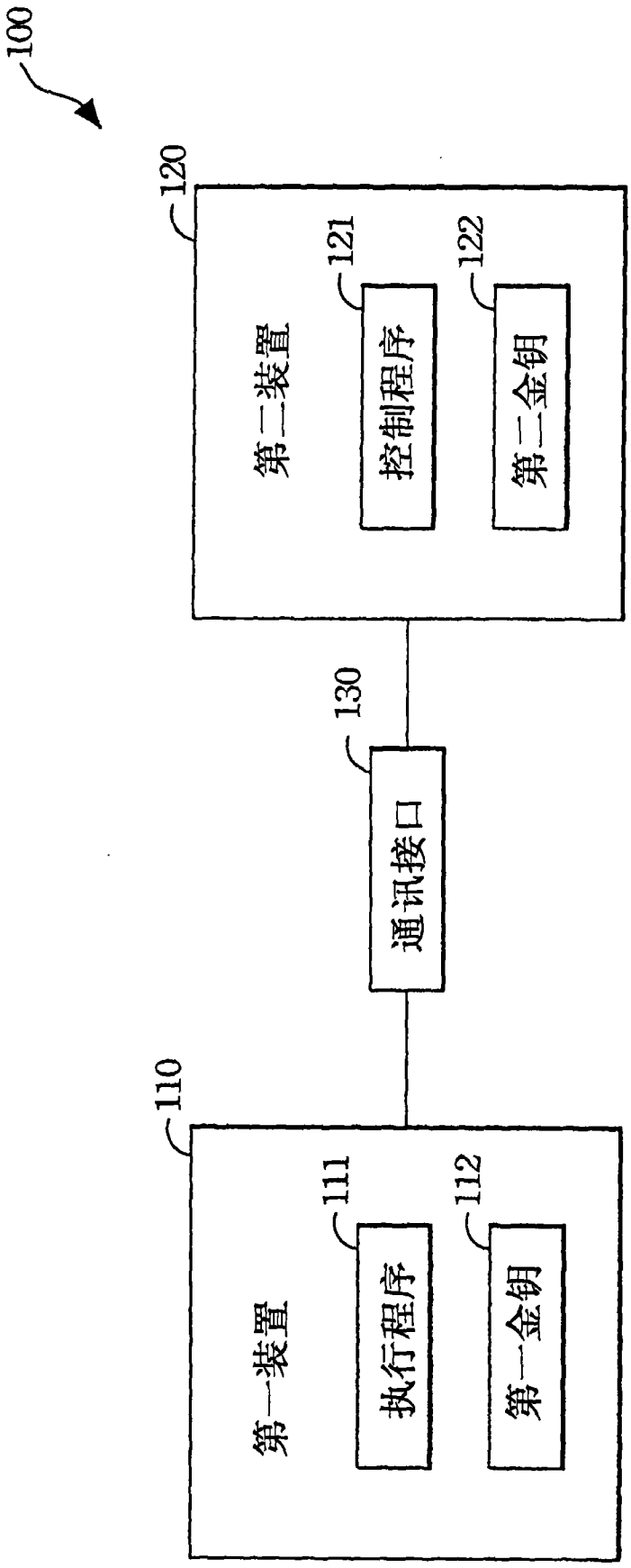

100
120
第二装置
121
控制程序
122
第二金钥
130
通讯接口
110
第一装置
111
执行程序
112
第一金钥

图1

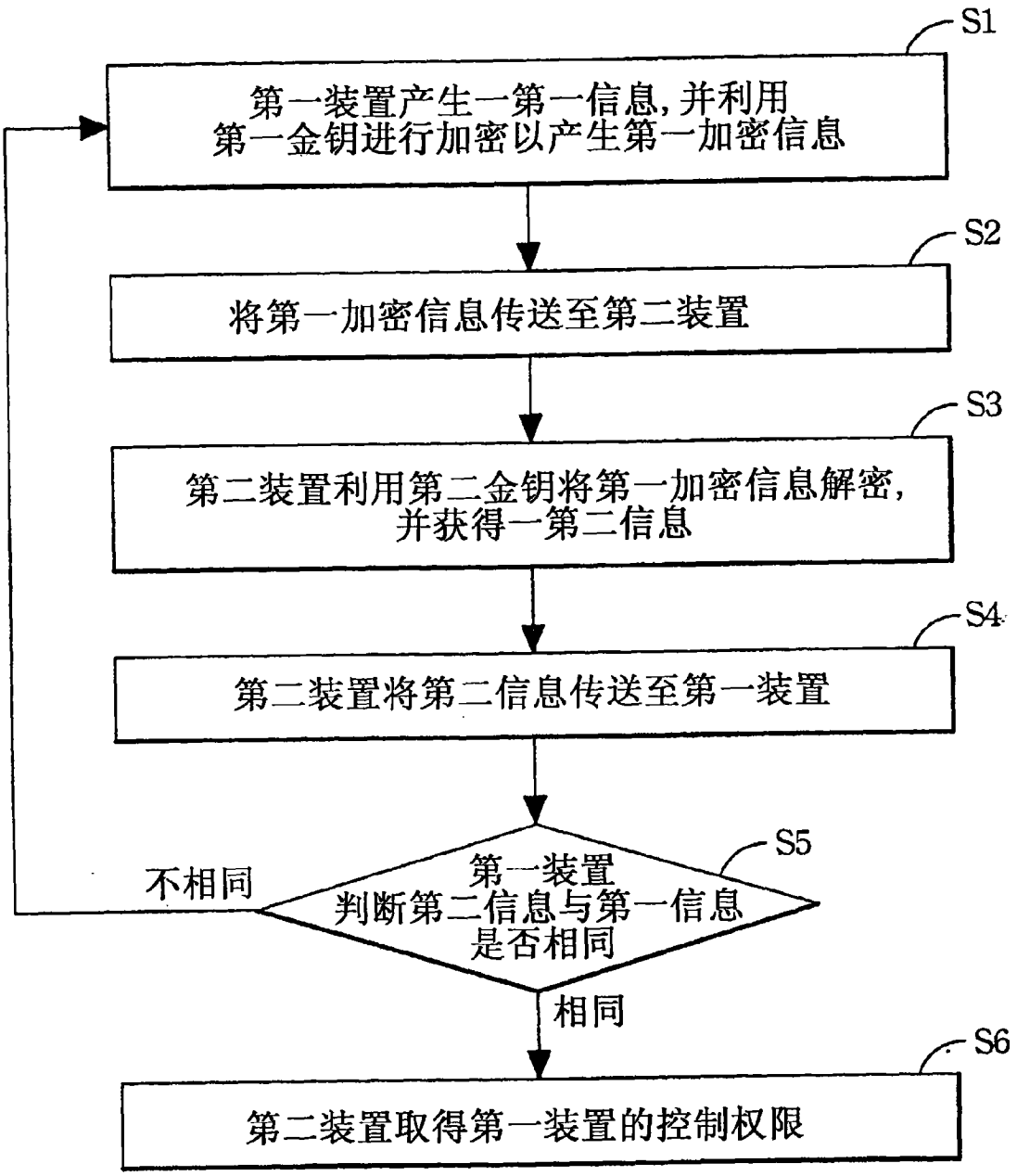

S1
第一装置产生一第一信息，并利用
第一金钥进行加密以产生第一加密信息
S2
将第一加密信息传送至第二装置
S3
第二装置利用第二金钥将第一加密信息解密，
并获得一第二信息
S4
第二装置将第二信息传送至第一装置
S5
第一装置
判断第二信息与第一信息
是否相同
不相同
相同
S6
第二装置取得第一装置的控制权限

图 2

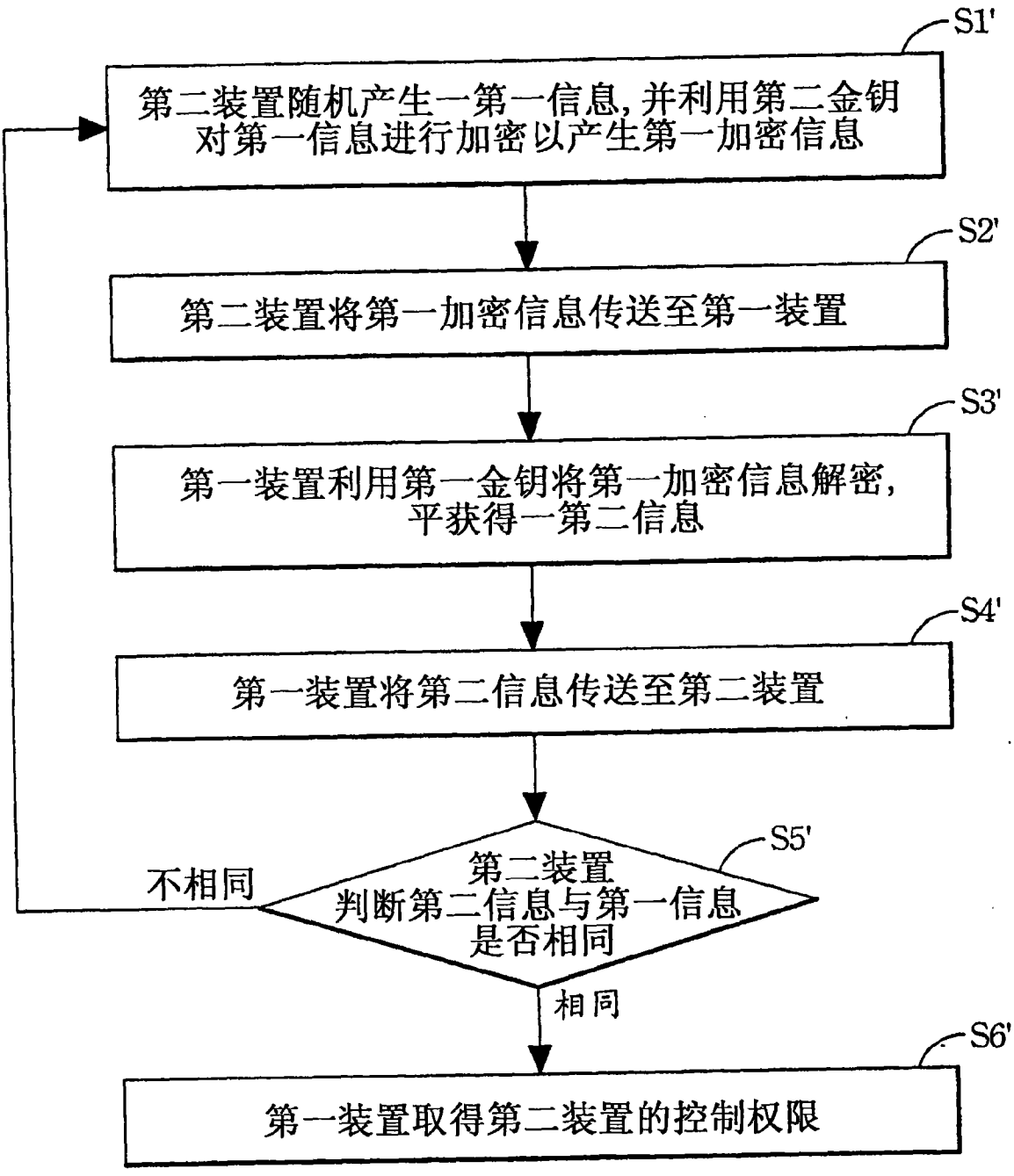

S1'
第二装置随机产生一第一信息，并利用第二金钥对第一信息进行加密以产生第一加密信息
S2'
第二装置将第一加密信息传送至第一装置
S3'
第一装置利用第一金钥将第一加密信息解密，平获得一第二信息
S4'
第一装置将第二信息传送至第二装置
S5'
第二装置判断第二信息与第一信息是否相同
不相同
相同
S6'
第一装置取得第二装置的控制权限

图 3