[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04N 7/16 (2006.01)
H04N 7/18 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810239858.8

[43] 公开日 2009 年 6 月 3 日

[11] 公开号 CN 101448130A

[22] 申请日 2008.12.19
[21] 申请号 200810239858.8
[71] 申请人 北京中星微电子有限公司
地址 100083 北京市海淀区学院路 35 号世宁大厦 15 层
[72] 发明人 邱 嵩 邓中翰 金兆玮 杨晓东

[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 王 琦 王诚华

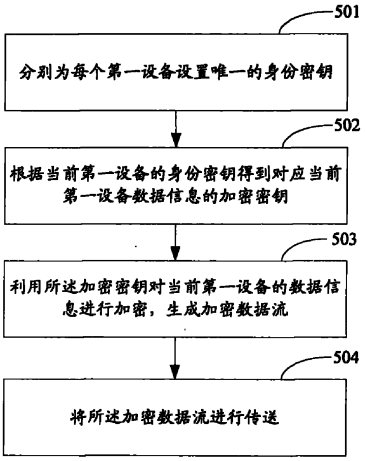
权利要求书 8 页 说明书 24 页 附图 5 页

[54] 发明名称

监控系统中数据加密保护的方法、系统和设备

[57] 摘要

本发明公开了一种监控系统中数据加密保护的方法，包括：分别为每个第一设备设置唯一的身份密钥；根据当前第一设备的身份密钥得到对应当前第一设备数据信息的加密密钥，利用所述加密密钥对当前第一设备的数据信息进行加密，生成加密数据流，将所述加密数据流进行传送。 此外，本发明还公开了一种支持数据加密保护的监控系统、监控中心和第一设备。 本发明所公开的技术方案能够提高数据信息的安全性。



1、一种监控系统中数据加密保护的方法，其特征在于，该方法包括:

分别为每个第一设备设置唯一的身份密钥;

根据当前第一设备的身份密钥得到对应当前第一设备数据信息的加密密钥，利用所述加密密钥对当前第一设备的数据信息进行加密，生成加密数据流，将所述加密数据流进行传送。

2、如权利要求 1 所述的方法，其特征在于，所述根据当前第一设备的身份密钥得到对应当前第一设备的加密密钥包括:

监控中心按照第一预设规则生成工作密钥，利用当前第一设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给当前第一设备;

当前第一设备利用自身的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥，将所述工作密钥作为对应当前第一设备数据信息的加密密钥。

3、如权利要求 1 所述的方法，其特征在于，所述根据当前第一设备的身份密钥得到对应当前第一设备的加密密钥包括:

监控中心按照第一预设规则生成工作密钥，利用当前第一设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给当前第一设备;

当前第一设备利用自身的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥，利用所述工作密钥和自身的身份密钥生成对应当前第一设备数据信息的加密密钥。

4、如权利要求 1 所述的方法，其特征在于，所述根据当前第一设备的身份密钥得到对应当前第一设备的加密密钥包括:

将所述身份密钥作为对应当前第一设备数据信息的加密密钥。

5、如权利要求 1 至 4 中任一项所述的方法，其特征在于，该方法进一步包括:

分别为每个第二设备设置唯一的身份密钥;

第二设备通过监控中心接收来自第一设备的加密数据流时，监控中心利用

所述第二设备的身份密钥对对应所述第一设备数据信息的加密密钥进行加密，将加密后的加密密钥发送给所述第二设备；

所述第二设备利用自身的身份密钥对所述加密后的加密密钥进行解密，得到所述加密密钥，利用所述加密密钥对所述第一设备的加密数据流进行解密，得到所述第一设备的数据信息。

6、如权利要求 5 所述的方法，其特征在于，所述第二设备在得到所述加密密钥后，进一步包括：对所述加密密钥进行缓存；

所述利用加密密钥对所述第一设备的加密数据流进行解密时，如果无法解开，则该方法进一步包括：利用自身缓存的时间邻近的其它加密密钥对所述第一设备的加密数据流进行解密。

7、如权利要求 5 所述的方法，其特征在于，该方法进一步包括：在所述加密数据流中的每个加密数据包中设置加密标志；

所述监控中心利用所述第二设备的身份密钥对对应所述第一设备数据信息的加密密钥进行加密之前，进一步包括：判断数据包中是否存在加密标志，如果存在，则执行所述利用所述第二设备的身份密钥对对应所述第一设备数据信息的加密密钥进行加密的操作；

所述第二设备利用加密密钥对所述第一设备的加密数据流进行解密之前，进一步包括：判断数据包中是否存在加密标志，如果存在，则执行所述利用加密密钥对所述第一设备的加密数据流进行解密的操作。

8、如权利要求 5 所述的方法，其特征在于，所述利用加密密钥对当前第一设备的数据信息进行加密包括：利用加密密钥对当前第一设备的原始数据信息进行加密；

或者包括：将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，利用加密密钥分别对每个原始数据单元中的数据载荷进行加密；

或者包括：将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，对每个原始数据单元按照第二预设规则产生认证数据，

将所述认证数据附加在对应原始数据单元的前面或后面，利用加密密钥分别对每个附加有认证数据的原始数据单元进行加密；此时，第二设备得到所述第一设备的数据信息之后，进一步包括：对所述数据信息进行认证处理。

9、如权利要求 1 所述的方法，其特征在于，所述根据当前第一设备的身份密钥得到对应当前第一设备的加密密钥包括：

监控中心按照第一预设规则生成工作密钥，利用当前第一设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给当前第一设备；

当前第一设备利用自身的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥，利用所述工作密钥和自身的身份密钥生成中间密钥，利用所述中间密钥与本地产生的对应每个加密数据包的随机密钥生成对应所述当前第一设备数据信息每个加密数据包的加密密钥。

10、如权利要求 9 所述的方法，其特征在于，所述加密数据流中对应每个加密数据包携带有对应的随机密钥；该方法进一步包括：

分别为每个第二设备设置唯一的身份密钥；

第二设备通过监控中心接收来自第一设备的加密数据流时，监控中心利用所述第二设备的身份密钥对对应所述第一设备数据信息的中间密钥进行加密，将加密后的中间密钥发送给所述第二设备；

所述第二设备利用自身的身份密钥对所述加密后的中间密钥进行解密，得到所述中间密钥，利用所述中间密钥及所述第一设备的加密数据流中对应每个加密数据包携带的随机密钥生成对应的加密数据包的加密密钥，利用所述加密密钥对对应的加密数据包进行解密，得到所述第一设备的数据信息。

11、如权利要求 10 所述的方法，其特征在于，所述利用加密密钥对当前第一设备的数据信息进行加密包括：将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，利用对应当前加密数据包的加密密钥对当前原始数据单元进行加密；

或者包括：将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，对每个原始数据单元按照第二预设规则产生认证数据，

将所述认证数据附加在对应原始数据单元的前面或后面，利用对应当前加密数据包的加密密钥对当前附加有认证数据的原始数据单元进行加密；此时，所述第二设备得到所述第一设备的数据信息之后，进一步包括：对所述数据信息进行认证处理。

12、如权利要求 10 所述的方法，其特征在于，所述第二设备在得到所述中间密钥后，进一步包括：对所述中间密钥进行缓存；

所述利用加密密钥对所述第一设备的加密数据流进行解密时，如果无法解开，则该方法进一步包括：利用自身缓存的时间邻近的其它中间密钥及所述第一设备的加密数据流中对应每个加密数据包携带的随机密钥生成对应的加密数据包的加密密钥，利用所述加密密钥对对应的加密数据包进行解密。

13、如权利要求 10 所述的方法，其特征在于，该方法进一步包括：在所述加密数据流中的每个加密数据包中设置加密标志；

所述监控中心利用所述第二设备的身份密钥对对应所述第一设备数据信息的中间密钥进行加密之前，进一步包括：判断数据包中是否存在加密标志，如果存在，则执行所述利用第二设备的身份密钥对对应所述第一设备数据信息的中间密钥进行加密的操作；

所述第二设备利用加密密钥对对应的加密数据包进行解密之前，进一步包括：判断数据包中是否存在加密标志，如果存在，则执行所述利用加密密钥对对应的加密数据包进行解密的操作。

14、如权利要求 10 所述的方法，其特征在于，所述利用加密密钥对当前第一设备的数据信息进行加密包括：利用加密密钥对当前第一设备的原始数据信息进行加密；

或者包括：将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，利用加密密钥分别对每个原始数据单元中的数据载荷进行加密；

或者包括：将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，对每个原始数据单元按照第二预设规则产生认证数据，

将所述认证数据附加在对应原始数据单元的前面或后面，利用加密密钥分别对每个附加有认证数据的原始数据单元进行加密；此时，第二设备得到所述第一设备的数据信息之后，进一步包括：对所述数据信息进行认证处理。

15、一种支持数据加密保护的监控系统，包括：第一设备、监控中心和第二设备，其特征在于，

所述监控中心用于存储分别为每个第一设备设置的唯一身份密钥，并按照第一预设规则生成工作密钥，利用当前第一设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给当前第一设备；

所述第一设备用于存储自身的身份密钥；接收来自监控中心的所述加密后的工作密钥，利用自身的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥，根据所述工作密钥得到对应当前数据信息的加密密钥，利用所述加密密钥对自身的数据信息进行加密，生成加密数据流，将所述加密数据流进行传送。

16、如权利要求 15 所述的系统，其特征在于，所述第一设备包括：

存储单元，用于存储自身所在第一设备的身份密钥；

接收单元，用于接收来自监控中心的加密后的工作密钥；

工作密钥解析单元，用于利用自身所在第一设备的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥；

加密密钥生成单元，用于将所述工作密钥作为对应自身所在第一设备数据信息的加密密钥；或者，利用所述工作密钥和自身所在第一设备的身份密钥生成对应自身所在第一设备数据信息的加密密钥；

加密单元，用于利用所述加密密钥对自身所在第一设备的数据信息进行加密。

17、如权利要求 16 所述的系统，其特征在于，所述监控中心进一步存储分别为每个第二设备设置的唯一身份密钥，在所述第二设备通过监控中心接收来自第一设备的加密数据流时，利用所述第二设备的身份密钥对对应所述第一设备数据信息的加密密钥进行加密，将加密后的加密密钥发送给所述第二设备；

所述第二设备用于通过监控中心接收来自第一设备的加密数据流，接收来自监控中心的加密后的加密密钥，利用自身的身份密钥对所述加密后的加密密钥进行解密，得到所述加密密钥，利用所述加密密钥对所述第一设备的加密数据流进行解密，得到所述第一设备的数据信息。

18、如权利要求 15 所述的系统，其特征在于，所述第一设备包括:

存储单元，用于存储自身所在第一设备的身份密钥;

接收单元，用于接收来自监控中心的加密后的工作密钥;

工作密钥解析单元，用于利用存储单元存储的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥;

中间密钥生成单元，用于利用所述工作密钥和自身所在第一设备的身份密钥生成中间密钥;

加密密钥生成单元，用于利用所述中间密钥与本地产生的对应每个加密数据包的随机密钥生成对应自身所在第一设备数据信息每个加密数据包的加密密钥;

加密单元，用于利用所述加密密钥对自身所在第一设备数据信息的对应数据包进行加密。

19、如权利要求 18 所述的系统，其特征在于，所述监控中心进一步存储分别为每个第二设备设置的唯一身份密钥，在所述第二设备通过监控中心接收来自第一设备的加密数据流时，利用所述第二设备的身份密钥对对应所述第一设备数据信息的中间密钥进行加密，将加密后的中间密钥发送给所述第二设备;

所述第二设备用于通过监控中心接收来自第一设备的加密数据流，接收来自监控中心的加密后的中间密钥，利用自身的身份密钥对所述加密后的中间密钥进行解密，得到所述中间密钥，利用所述中间密钥及所述第一设备的加密数据流中对应每个加密数据包携带的随机密钥生成对应的加密数据包的加密密钥，利用所述加密密钥对对应的加密数据包进行解密，得到所述第一设备的数据信息。

20、一种监控中心，其特征在于，该监控中心包括:

数据处理单元，用于接收前端设备对监控信息加密后的加密数据流，根据被授权访问所述前端设备监控信息的后端设备的请求，将所述加密数据流发送给所述后端设备；

安全管理单元，用于存储分别为每个前端设备和后端设备设置的唯一身份密钥，并按照第一预设规则生成工作密钥，在前端设备对自身监控信息进行编码时，利用所述前端设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给所述前端设备；在数据处理单元将前端设备的加密数据流发送给后端设备时，利用所述后端设备的身份密钥对对应所述前端设备监控信息的加密密钥或中间密钥进行加密，将加密后的加密密钥或中间密钥发送给所述后端设备。

21、如权利要求 20 所述的监控中心，其特征在于，所述数据处理单元进一步接收被授权控制设定前端设备的后端设备对控制信息加密后的加密数据流，将所述加密数据流发送给对应的前端设备；

安全管理单元进一步在后端设备需要对发送给前端设备的控制信息进行加密时，利用所述后端设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给所述后端设备；在数据处理单元将后端设备的加密数据流发送给前端设备时，利用所述前端设备的身份密钥对对应所述后端设备控制信息的加密密钥或中间密钥进行加密，将加密后的加密密钥或中间密钥发送给所述前端设备。

22、一种第一设备，其特征在于，该设备包括：

存储单元，用于存储自身所在第一设备的身份密钥；

接收单元，用于接收来自监控中心的加密后的工作密钥；

工作密钥解析单元，用于利用自身所在第一设备的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥；

加密密钥生成单元，用于将所述工作密钥作为对应自身所在第一设备数据信息的加密密钥；或者，利用所述工作密钥和自身所在第一设备的身份密钥生成对应自身所在第一设备数据信息的加密密钥；

加密单元，用于利用所述加密密钥对自身所在第一设备的数据信息进行加密。

23、一种第一设备，其特征在于，该设备包括:

存储单元，用于存储自身所在第一设备的身份密钥;

接收单元，用于接收来自监控中心的加密后的工作密钥;

工作密钥解析单元，用于利用存储单元存储的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥;

中间密钥生成单元，用于利用所述工作密钥和自身所在第一设备的身份密钥生成中间密钥;

加密密钥生成单元，用于利用所述中间密钥与本地产生的对应每个加密数据包的随机密钥生成对应自身所在第一设备数据信息每个加密数据包的加密密钥;

加密单元，用于利用所述加密密钥对自身所在第一设备数据信息的对应数据包进行加密。

监控系统中数据加密保护的方法、系统和设备

技术领域

本发明涉及监控系统，尤其涉及一种监控系统中数据加密保护的方法、支持数据加密保护的监控系统和设备。

背景技术

在监控系统中，主要包括前端设备、后端设备和监控中心。其中，前端设备主要包括音频、视频等监控信息采集、编码的设备，后端设备主要包括音频、视频等监控信息解码、显示、播放和存储，以及对前端设备进行控制的设备，如对摄像头的云台动作控制、摄像头的镜头伸缩控制以及摄像头的参数调整等的设备。监控中心为系统的整体管理中心，也称中心平台服务器，主要负责设备接入和信令传输等监控业务功能，以及媒体流的传输和存储等功能。具体实现时，监控中心可由多个分别负责不同功能的服务器组成。

在监控应用中，各种与监控相关的信息，如包括音视频、报警等在内的监控信息和控制信息等的安全性非常重要。但现有技术中，前端设备通过监控中心发送给后端设备的监控信息、以及后端设备通过监控中心发送给前端设备的控制信息均是没有加密过的数据，其中的监控信息也只是在传输过程中进行了网络层的加密，而对于前端设备本地存储的监控数据及监控中心存储的监控数据均是没有加密过的数据。可见，现有技术中监控信息和控制信息均存在被恶意获取的可能性，安全性较低。

发明内容

有鉴于此，本发明中一方面提供一种监控系统中数据加密保护的方法，另一方面提供一种支持数据加密保护的监控系统、监控中心和第一设备，以便提高数据信息的安全性。

本发明所提供的监控系统中数据加密保护的方法，包括：

分别为每个第一设备设置唯一的身份密钥；

根据当前第一设备的身份密钥得到对应当前第一设备数据信息的加密密钥，利用所述加密密钥对当前第一设备的数据信息进行加密，生成加密数据流，将所述加密数据流进行传送。

较佳地，所述根据当前第一设备的身份密钥得到对应当前第一设备的加密密钥包括：

监控中心按照第一预设规则生成工作密钥，利用当前第一设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给当前第一设备；

当前第一设备利用自身的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥，将所述工作密钥作为对应当前第一设备数据信息的加密密钥。

较佳地，所述根据当前第一设备的身份密钥得到对应当前第一设备的加密密钥包括：

监控中心按照第一预设规则生成工作密钥，利用当前第一设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给当前第一设备；

当前第一设备利用自身的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥，利用所述工作密钥和自身的身份密钥生成对应当前第一设备数据信息的加密密钥。

较佳地，所述根据当前第一设备的身份密钥得到对应当前第一设备的加密密钥包括：

将所述身份密钥作为对应当前第一设备数据信息的加密密钥。

较佳地，该方法进一步包括：

分别为每个第二设备设置唯一的身份密钥；

第二设备通过监控中心接收来自第一设备的加密数据流时，监控中心利用所述第二设备的身份密钥对对应所述第一设备数据信息的加密密钥进行加密，将加密后的加密密钥发送给所述第二设备；

所述第二设备利用自身的身份密钥对所述加密后的加密密钥进行解密，得

到所述加密密钥，利用所述加密密钥对所述第一设备的加密数据流进行解密，得到所述第一设备的数据信息。

较佳地，所述第二设备在得到所述加密密钥后，进一步包括：对所述加密密钥进行缓存；

所述利用加密密钥对所述第一设备的加密数据流进行解密时，如果无法解开，则该方法进一步包括：利用自身缓存的时间邻近的其它加密密钥对所述第一设备的加密数据流进行解密。

较佳地，该方法进一步包括：在所述加密数据流中的每个加密数据包中设置加密标志；

所述监控中心利用所述第二设备的身份密钥对对应所述第一设备数据信息的加密密钥进行加密之前，进一步包括：判断数据包中是否存在加密标志，如果存在，则执行所述利用所述第二设备的身份密钥对对应所述第一设备数据信息的加密密钥进行加密的操作；

所述第二设备利用加密密钥对所述第一设备的加密数据流进行解密之前，进一步包括：判断数据包中是否存在加密标志，如果存在，则执行所述利用加密密钥对所述第一设备的加密数据流进行解密的操作。

较佳地，所述利用加密密钥对当前第一设备的数据信息进行加密包括：利用加密密钥对当前第一设备的原始数据信息进行加密；

或者包括：将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，利用加密密钥分别对每个原始数据单元中的数据载荷进行加密；

或者包括：将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，对每个原始数据单元按照第二预设规则产生认证数据，将所述认证数据附加在对应原始数据单元的前面或后面，利用加密密钥分别对每个附加有认证数据的原始数据单元进行加密；此时，第二设备得到所述第一设备的数据信息之后，进一步包括：对所述数据信息进行认证处理。

较佳地，所述根据当前第一设备的身份密钥得到对应当前第一设备的加密

密钥包括:

监控中心按照第一预设规则生成工作密钥，利用当前第一设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给当前第一设备;

当前第一设备利用自身的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥，利用所述工作密钥和自身的身份密钥生成中间密钥，利用所述中间密钥与本地产生的对应每个加密数据包的随机密钥生成对应所述当前第一设备数据信息每个加密数据包的加密密钥。

较佳地，所述加密数据流中对应每个加密数据包携带有对应的随机密钥;该方法进一步包括:

分别为每个第二设备设置唯一的身份密钥;

第二设备通过监控中心接收来自第一设备的加密数据流时，监控中心利用所述第二设备的身份密钥对对应所述第一设备数据信息的中间密钥进行加密，将加密后的中间密钥发送给所述第二设备;

所述第二设备利用自身的身份密钥对所述加密后的中间密钥进行解密，得到所述中间密钥，利用所述中间密钥及所述第一设备的加密数据流中对应每个加密数据包携带的随机密钥生成对应的加密数据包的加密密钥，利用所述加密密钥对对应的加密数据包进行解密，得到所述第一设备的数据信息。

较佳地，所述利用加密密钥对当前第一设备的数据信息进行加密包括：将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，利用对应当前加密数据包的加密密钥对当前原始数据单元进行加密;

或者包括：将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，对每个原始数据单元按照第二预设规则产生认证数据，将所述认证数据附加在对应原始数据单元的前面或后面，利用对应当前加密数据包的加密密钥对当前附加有认证数据的原始数据单元进行加密；此时，所述第二设备得到所述第一设备的数据信息之后，进一步包括：对所述数据信息进行认证处理。

较佳地，所述第二设备在得到所述中间密钥后，进一步包括：对所述中间

密钥进行缓存；

所述利用加密密钥对所述第一设备的加密数据流进行解密时，如果无法解开，则该方法进一步包括：利用自身缓存的时间邻近的其它中间密钥及所述第一设备的加密数据流中对应每个加密数据包携带的随机密钥生成对应的加密数据包的加密密钥，利用所述加密密钥对对应的加密数据包进行解密。

较佳地，该方法进一步包括：在所述加密数据流中的每个加密数据包中设置加密标志；

所述监控中心利用所述第二设备的身份密钥对对应所述第一设备数据信息的中间密钥进行加密之前，进一步包括：判断数据包中是否存在加密标志，如果存在，则执行所述利用第二设备的身份密钥对对应所述第一设备数据信息的中间密钥进行加密的操作；

所述第二设备利用加密密钥对对应的加密数据包进行解密之前，进一步包括：判断数据包中是否存在加密标志，如果存在，则执行所述利用加密密钥对对应的加密数据包进行解密的操作。

较佳地，所述利用加密密钥对当前第一设备的数据信息进行加密包括：利用加密密钥对当前第一设备的原始数据信息进行加密；

或者包括：将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，利用加密密钥分别对每个原始数据单元中的数据载荷进行加密；

或者包括：将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，对每个原始数据单元按照第二预设规则产生认证数据，将所述认证数据附加在对应原始数据单元的前面或后面，利用加密密钥分别对每个附加有认证数据的原始数据单元进行加密；此时，第二设备得到所述第一设备的数据信息之后，进一步包括：对所述数据信息进行认证处理。

本发明所提供的支持数据加密保护的监控系统，包括：第一设备、监控中心和第二设备，其中，

所述监控中心用于存储分别为每个第一设备设置的唯一身份密钥，并按照

第一预设规则生成工作密钥，利用当前第一设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给当前第一设备；

所述第一设备用于存储自身的身份密钥；接收来自监控中心的所述加密后的工作密钥，利用自身的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥，根据所述工作密钥得到对应当前数据信息的加密密钥，利用所述加密密钥对自身的数据信息进行加密，生成加密数据流，将所述加密数据流进行传送。

较佳地，所述第一设备包括：

存储单元，用于存储自身所在第一设备的身份密钥；

接收单元，用于接收来自监控中心的加密后的工作密钥；

工作密钥解析单元，用于利用自身所在第一设备的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥；

加密密钥生成单元，用于将所述工作密钥作为对应自身所在第一设备数据信息的加密密钥；或者，利用所述工作密钥和自身所在第一设备的身份密钥生成对应自身所在第一设备数据信息的加密密钥；

加密单元，用于利用所述加密密钥对自身所在第一设备的数据信息进行加密。

较佳地，所述监控中心进一步存储分别为每个第二设备设置的唯一身份密钥，在所述第二设备通过监控中心接收来自第一设备的加密数据流时，利用所述第二设备的身份密钥对对应所述第一设备数据信息的加密密钥进行加密，将加密后的加密密钥发送给所述第二设备；

所述第二设备用于通过监控中心接收来自第一设备的加密数据流，接收来自监控中心的加密后的加密密钥，利用自身的身份密钥对所述加密后的加密密钥进行解密，得到所述加密密钥，利用所述加密密钥对所述第一设备的加密数据流进行解密，得到所述第一设备的数据信息。

较佳地，所述第一设备包括：

存储单元，用于存储自身所在第一设备的身份密钥；

接收单元，用于接收来自监控中心的加密后的工作密钥；

工作密钥解析单元，用于利用存储单元存储的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥；

中间密钥生成单元，用于利用所述工作密钥和自身所在第一设备的身份密钥生成中间密钥；

加密密钥生成单元，用于利用所述中间密钥与本地产生的对应每个加密数据包的随机密钥生成对应自身所在第一设备数据信息每个加密数据包的加密密钥；

加密单元，用于利用所述加密密钥对自身所在第一设备数据信息的对应数据包进行加密。

较佳地，所述监控中心进一步存储分别为每个第二设备设置的唯一身份密钥，在所述第二设备通过监控中心接收来自第一设备的加密数据流时，利用所述第二设备的身份密钥对对应所述第一设备数据信息的中间密钥进行加密，将加密后的中间密钥发送给所述第二设备；

所述第二设备用于通过监控中心接收来自第一设备的加密数据流，接收来自监控中心的加密后的中间密钥，利用自身的身份密钥对所述加密后的中间密钥进行解密，得到所述中间密钥，利用所述中间密钥及所述第一设备的加密数据流中对应每个加密数据包携带的随机密钥生成对应的加密数据包的加密密钥，利用所述加密密钥对对应的加密数据包进行解密，得到所述第一设备的数据信息。

本发明所提供的监控中心，包括：

数据处理单元，用于接收前端设备对监控信息加密后的加密数据流，根据被授权访问所述前端设备监控信息的后端设备的请求，将所述加密数据流发送给所述后端设备；

安全管理单元，用于存储分别为每个前端设备和后端设备设置的唯一身份密钥，并按照第一预设规则生成工作密钥，在前端设备对自身监控信息进行编码时，利用所述前端设备的身份密钥对当前生成的工作密钥进行加密，将加密

后的工作密钥发送给所述前端设备；在数据处理单元将前端设备的加密数据流发送给后端设备时，利用所述后端设备的身份密钥对对应所述前端设备监控信息的加密密钥或中间密钥进行加密，将加密后的加密密钥或中间密钥发送给所述后端设备。

较佳地，所述数据处理单元进一步接收被授权控制设定前端设备的后端设备对控制信息加密后的加密数据流，将所述加密数据流发送给对应的前端设备；

安全管理单元进一步在后端设备需要对发送给前端设备的控制信息进行加密时，利用所述后端设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给所述后端设备；在数据处理单元将后端设备的加密数据流发送给前端设备时，利用所述前端设备的身份密钥对对应所述后端设备控制信息的加密密钥或中间密钥进行加密，将加密后的加密密钥或中间密钥发送给所述前端设备。

本发明所提供的第一设备，包括：

存储单元，用于存储自身所在第一设备的身份密钥；

接收单元，用于接收来自监控中心的加密后的工作密钥；

工作密钥解析单元，用于利用自身所在第一设备的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥；

加密密钥生成单元，用于将所述工作密钥作为对应自身所在第一设备数据信息的加密密钥；或者，利用所述工作密钥和自身所在第一设备的身份密钥生成对应自身所在第一设备数据信息的加密密钥；

加密单元，用于利用所述加密密钥对自身所在第一设备的数据信息进行加密。

本发明所提供的又一种第一设备，包括：

存储单元，用于存储自身所在第一设备的身份密钥；

接收单元，用于接收来自监控中心的加密后的工作密钥；

工作密钥解析单元，用于利用存储单元存储的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥；

中间密钥生成单元，用于利用所述工作密钥和自身所在第一设备的身份密钥生成中间密钥；

加密密钥生成单元，用于利用所述中间密钥与本地产生的对应每个加密数据包的随机密钥生成对应自身所在第一设备数据信息每个加密数据包的加密密钥；

加密单元，用于利用所述加密密钥对自身所在第一设备数据信息的对应数据包进行加密。

从上述方案可以看出，本发明中通过分别为每个第一设备，如前端设备或后端设备设置唯一的身份密钥，并根据当前第一设备，如前端设备或后端设备的身份密钥得到对应当前第一设备数据信息，如前端设备的监控信息或后端设备的控制信息的加密密钥，利用所述加密密钥对当前第一设备的数据信息，如前端设备的监控信息或后端设备的控制信息进行加密，生成加密数据流，将所述加密数据流进行传送，从而提高了数据信息的安全性。

上述根据当前第一设备，如前端设备或后端设备的身份密钥得到对应当前第一设备数据信息，如前端设备的监控信息或后端设备的控制信息的加密密钥的方式可以有多种，可以直接将第一设备的身份密钥或监控中心分配的工作密钥作为加密密钥，即一级密钥，也可以利用所述工作密钥和第一设备的身份密钥生成加密密钥，即二级密钥，此外，还可以利用所述工作密钥和第一设备的身份密钥生成中间密钥，利用所述中间密钥与第一设备本地产生的对应每个加密数据包的随机密钥生成对应第一设备数据信息每个加密数据包的加密密钥，即三级密钥。其中，密钥级数越高，则数据信息的安全性越高。

其中，数据信息传输给监控中心时，由于监控中心中存储有第一设备的身份密钥，因此能够获知加密数据流中各加密数据包对应的加密密钥，进而可对该加密数据流进行解密，将解密后的数据信息发送给第二设备，如后端设备或前端设备。或者，进一步地，若第二设备，如后端设备或前端设备也接收加密数据流，则监控中心中还存储有第二设备的身份密钥，此时可利用

第二设备的身份密钥对对应所述第一设备数据信息的加密密钥或中间密钥进行加密，将加密后的加密密钥或中间密钥发送给所述第二设备，然后第二设备利用自身的身份密钥对所述加密后的加密密钥或中间密钥进行解密，得到所述加密密钥或中间密钥，利用所述加密密钥或利用所述中间密钥及所述第一设备的加密数据流中对应每个加密数据包携带的随机密钥生成对应的加密数据包的加密密钥对所述第一设备的加密数据流进行解密，得到所述第一设备的数据信息，从而进一步提高了数据信息的安全性。

此外，通过对数据增加认证处理，可以在提高数据安全性的同时，提供数据的完整性和真实性保护。

另外，由于工作密钥是不断更新的，如周期更新等，因此通过在解密端，即第二设备缓存多组工作密钥（如三组工作密钥 W: W_{N-1}，W_N，W_{N+1}，分别对应过去、现在和将来采用的工作密钥），解密端接收到加密数据后，如果用其中一个密钥解密得到的结果不对，可以先尝试用其它密钥解密，避免了由于网络延时等原因造成的密钥更新不同步问题，保证了不断更新的工作密钥 W 在各个设备之间的同步。

最后，通过在加密数据包中，如加密数据包的包头中设置加密标志，使得的加密端可以在识别出有该加密标志时，对数据包进行解密，否则按现有技术进行处理，从而使得本发明中的监控系统能够与现有技术中的前端设备实现兼容。

附图说明

图 1 为本发明实施例中支持数据加密保护的监控系统的结构示意图；

图 2a 至图 2d 为本发明实施例中数据加密的各种示意图；

图 3a 至图 3c 为本发明实施例中第一设备的各种结构示意图；

图 4a 和图 4b 为本发明实施例中第二设备的各种结构示意图；

图 5 为本发明实施例中监控系统中数据加密保护的方法流程示意图。

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明白，下面结合实施例和附图，对本发明进一步详细说明。

图 1 为本发明实施例中支持数据加密保护的监控系统的结构示意图。如图 1 所示，该系统包括：前端设备、监控中心和后端设备。

其中，前端设备用于将自身采集、加密后的监控信息发送给监控中心，由监控中心根据后端设备对选定前端设备的访问请求，判断所述后端设备是否被授权访问所述选定前端设备的监控信息，如果是，则将所述选定前端设备的监控信息发送给后端设备。

后端设备用于接收通过监控中心转发的前端设备的监控信息，对所述监控信息进行显示、播放或存储等操作。

此外，由于后端设备还用于对被授权控制的前端设备进行控制，因此后端设备可向监控中心发送用于控制前端设备的控制信息，由监控中心将该控制信息转发给对应的前端设备，控制该前端设备完成相应的操作。

由于本发明实施例中将要描述的技术方案既可应用于对监控信息的加密保护，也可以应用于对控制信息的加密保护，具体应用于二者之一还是二者都应用，则可由使用者根据实际需要确定。而监控信息是由前端设备发出，后端设备接收，控制信息是由后端设备发出，前端设备接收。因此，为描述方便，本发明实施例中，将数据信息（无论是监控信息还是控制信息）的发出端称为第一设备，将数据信息（无论是监控信息还是控制信息）的接收端称为第二设备。

本发明实施例中可首先对第一设备发送给监控中心的数据信息进行加密保护，则监控中心可对接收的第一设备的数据信息进行解密后发送给第二设备；或者，进一步地，也可对监控中心发送给第二设备的数据信息进行加密，此时，监控中心可直接将第一设备的加密后的数据信息发送给第二设备，然后第二设备对所接收的数据信息进行解密。

具体实现时，若只对第一设备发送给监控中心的数据信息进行加密，则可预先为每个第一设备分别设置一个唯一的身份密钥，并将该身份密钥分别存储在监控中心和对应的第一设备中。则具体进行加密时，可有多种具体实现形式，下面列举其中几种：

第一种：加密密钥为一级密钥。

第一设备可直接将自身的身份密钥（ID-Key）作为加密密钥对自身的数据信息进行加密，生成加密数据流，将所生成的加密数据流发送给监控中心；监控中心接收到所述加密数据流后，利用自身存储的该第一设备的身份密钥对所述加密数据流进行解密，得到该第一设备的数据信息。

第二种：加密密钥为一级密钥。

监控中心按照第一预设规则生成工作密钥（W-Key），如按照预设周期生成周期变化的工作密钥，然后利用自身存储的当前第一设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给当前第一设备。

第一设备接收来自监控中心的所述加密后的工作密钥，利用自身的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥，将所述工作密钥作为加密密钥对自身的数据信息进行加密，生成加密数据流，将所生成的加密数据流发送给监控中心。

监控中心在接收到当前第一设备的加密数据流后，利用发送给第一设备的工作密钥，即加密密钥，对所述加密数据流进行解密，得到该第一设备的数据信息。

第三种：加密密钥为二级密钥。

监控中心按照第一预设规则生成工作密钥，如按照预设周期生成周期变化的工作密钥，然后利用自身存储的当前第一设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给当前第一设备。

第一设备接收来自监控中心的所述加密后的工作密钥，利用自身的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥，利用所述工作密钥和自身的身份密钥按照第一密钥生成算法生成加密密钥，利用所生成的

加密密钥对自身的数据信息进行加密，生成加密数据流，将所生成的加密数据流发送给监控中心。

监控中心在接收到当前第一设备的加密数据流后，利用发送给第一设备的工作密钥及自身存储的该第一设备的身份密钥按照第一密钥生成算法生成加密密钥，利用所生成的加密密钥对所述加密数据流进行解密，得到该第一设备的数据信息。

第四种：加密密钥为三级密钥。

监控中心按照第一预设规则生成工作密钥，如按照预设周期生成周期变化的工作密钥，然后利用自身存储的当前第一设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给当前第一设备。

第一设备接收来自监控中心的所述加密后的工作密钥，利用自身的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥，利用所述工作密钥和自身的身份密钥按照第二密钥生成算法生成中间密钥，利用所述中间密钥与本地产生的对应每个加密数据包的随机密钥（T-Key）按照第三密钥生成算法生成对应数据信息每个加密数据包的加密密钥，利用所生成的加密密钥对自身数据信息的每个数据包进行加密，并且随机密钥随对应的加密数据包一起传送，生成加密数据流，将所生成的加密数据流发送给监控中心。其中，随机密钥可以是第一设备按照预设的算法每个加密数据包更新一次，并随加密数据一起传输（随机密钥 T-Key 是明文传输的，本身并不加密）。

监控中心在接收到当前第一设备的加密数据流后，利用发送给第一设备的工作密钥及自身存储的该第一设备的身份密钥按照第二密钥生成算法生成中间密钥，利用所生成的中间密钥及该第一设备的加密数据流中每个加密数据包携带的随机密钥按照第三密钥生成算法生成对应加密数据包的加密密钥，利用所述加密密钥对对应的加密数据包进行解密，得到该第一设备的数据信息。

上述四种方法中，均是根据第一设备的身份密钥得到的加密密钥。其中，后三种方法中还根据工作密钥得到加密密钥。

若还需对监控中心发送给第二设备的数据信息进行加密，则还可预先为每个第二设备分别设置一个唯一的身份密钥，并将该身份密钥分别存储在监控中心和对应的第二设备中。则具体实现时，对应上述四种情况，监控中心和第二设备还需进行如下处理：

对应第一至第三种情况：

监控中心进一步向第二设备发送来自第一设备的加密数据流，并利用该第二设备的身份密钥对对应该第一设备数据信息的加密密钥进行加密，将加密后的加密密钥发送给所述第二设备。其中，对应第一种情况，加密密钥为第一设备的身份密钥；对应第二种情况，加密密钥是发送给第一设备的工作密钥；对应第三种情况，加密密钥是利用第一设备的身份密钥和发送给第一设备的工作密钥按照第一密钥生成算法得到的加密密钥。

第二设备用于通过监控中心接收来自第一设备的加密数据流，接收来自监控中心的加密后的加密密钥，利用自身的身份密钥对所述加密后的加密密钥进行解密，得到所述加密密钥，利用所述加密密钥对所述第一设备的加密数据流进行解密，得到所述第一设备的数据信息。

对应第四种情况：

监控中心进一步向第二设备发送来自第一设备的加密数据流，并利用该第二设备的身份密钥对对应所述第一设备数据信息的中间密钥进行加密，将加密后的中间密钥发送给所述第二设备。

第二设备用于通过监控中心接收来自第一设备的加密数据流，接收来自监控中心的加密后的中间密钥，利用自身的身份密钥对所述加密后的中间密钥进行解密，得到所述中间密钥，利用所述中间密钥及所述第一设备的加密数据流中每个加密数据包携带的随机密钥按照第三密钥生成算法生成对应加密数据包的加密密钥，利用所述加密密钥对对应的加密数据包进行解密，得到所述第一设备的数据信息。

对于上述前三种情况，利用加密密钥对当前第一设备的数据信息进行加密时，加密对象可以是原始的数据信息，例如，对于监控信息来说，可以对

原始的数据信息，如音视频数据及其附属信息进行加密；也可以是将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元之后，对每个原始数据单元的数据载荷进行加密。如图 2a 所示，对按照网络传输协议要求封装的各原始数据单元（如 RDU1~RDUn）的数据载荷进行加密后，得到各加密后的数据单元（如 EDU1~EDUn）。

进一步的，为同时提供数据的完整性和真实性保护，防止数据被篡改，可对数据增加认证处理，如图 2b 所示，对每个原始数据单元按照第二预设规则产生认证数据（HMAC），附加在原始数据单元后面（或者，也可将认证数据附加在原始数据单元前面），再对由原始数据单元（RDU）和认证数据（HMAC）组成的数据单元加密。此时，监控中心或第二设备得到所述第一设备的数据信息之后，进一步包括：对所述数据信息进行认证处理的过程。认证处理可以采用通用的 MD5、SHA-1/256/384/512、HMAC 算法，也可以采用特定的算法。其中，具体认证处理过程可以是：监控中心或第二设备对第一设备数据信息的每个原始数据单元按照第二预设规则产生认证数据，将所述认证数据与对应原始数据单元后面或前面的认证数据进行匹配，如果相匹配，则确定认证通过，表明数据是完整真实的；否则，认证不通过，数据发生错误。

对于上述的第四种情况，加密对象为每个数据单元。例如，可以是将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，然后利用对应当前加密数据包的加密密钥对当前原始数据单元进行加密，得到加密后的加密数据单元，如图 2c 所示，同时随机密钥（T-Key）以明文的方式随对应的加密数据包（即加密数据单元）一起传输。

同样，为同时提供数据的完整性和真实性保护，防止数据被篡改，也可以增加认证数据，如图 2d 所示，对每个原始数据单元按照第二预设规则产生认证数据，将所述认证数据附加在对应原始数据单元的后面（或前面），利用对应当前加密数据包的加密密钥对当前附加有认证数据的原始数据单元进行加密，得到对应的加密数据单元，同时随机密钥（T-Key）以明文的

方式随对应的加密数据包（即加密数据单元）一起传输。此时，所述第二设备得到所述第一设备的数据信息之后，进一步包括：对所述数据信息进行认证处理。具体认证处理过程可以是：第二设备对第一设备数据信息的每个原始数据单元按照第二预设规则产生认证数据，将所述认证数据与对应原始数据单元后面或前面的认证数据进行匹配，如果相匹配，则确定认证通过，表明数据是完整真实的；否则，认证不通过，数据发生错误。

具体实现时，第一设备可有多种内部结构的实现形式，下面分别针对上述几种情况，对第一设备的内部实现进行详细描述。

对应上述第一种情况，第一设备的内部结构可如图 3a 所示，包括：存储单元、加密单元和发送单元。

其中，存储单元用于存储自身所在第一设备的身份密钥。

加密单元用于利用存储单元存储的身份密钥作为加密密钥对自身所在第一设备的数据信息进行加密。

发送单元用于将加密后的数据发送给监控中心。

对应第二和第三种情况，第一设备的内部结构可如图 3b 所示，包括：存储单元、接收单元、工作密钥解析单元、加密密钥生成单元、加密单元和发送单元。

其中，存储单元用于存储自身所在第一设备的身份密钥。

接收单元用于接收来自监控中心的加密后的工作密钥。

工作密钥解析单元用于利用自身所在第一设备的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥。

加密密钥生成单元用于将所述工作密钥作为对应自身所在第一设备数据信息的加密密钥；或者，利用所述工作密钥和自身所在第一设备的身份密钥按照第一密钥生成算法生成对应自身所在第一设备数据信息的加密密钥。

加密单元用于利用所述加密密钥对自身所在第一设备的数据信息进行加密。

发送单元用于将加密后的数据发送给监控中心。

对应第四种情况，第一设备的内部结构可如图 3c 所示，包括：存储单元、接收单元、工作密钥解析单元、中间密钥生成单元、加密密钥生成单元、加密单元和发送单元。

其中，存储单元用于存储自身所在第一设备的身份密钥。

接收单元用于接收来自监控中心的加密后的工作密钥。

工作密钥解析单元用于利用存储单元存储的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥。

中间密钥生成单元用于利用所述工作密钥和自身所在第一设备的身份密钥按照第二密钥生成算法生成中间密钥。

加密密钥生成单元用于利用所述中间密钥与本地产生的对应每个加密数据包的随机密钥按照第三密钥生成算法生成对应自身所在第一设备数据信息每个加密数据包的加密密钥。

加密单元，用于利用所述加密密钥对自身所在第一设备数据信息的对应数据包进行加密。

发送单元用于将加密后的数据发送给监控中心。

进一步地，第一设备中还可包括认证设置单元（图中未示出），用于对自身所在第一设备数据信息的每个原始数据单元按照第二预设规则产生认证数据，将所述认证数据附加在对应原始数据单元的后面或前面。则加密单元用于利用所述加密密钥对当前附加有认证数据的原始数据单元进行加密。

具体实现时，第二设备同样可有多种内部结构的实现形式，下面分别针对上述几种情况，对第二设备的内部实现进行详细描述。

对应上述第一至第三种情况，第二设备的内部结构可如图 4a 所示，包括：接收单元、加密密钥解析单元和解密单元。

其中，接收单元用于接收监控中心转发的来自第一设备的加密数据流，以及监控中心发送的对应第一设备数据信息的加密后的加密密钥。

加密密钥解析单元用于利用自身所在第二设备的身份密钥对接收单元接收的所述加密密钥进行解密，得到对应第一设备数据信息的加密密钥。

解密单元用于利用加密密钥解析单元解析出的所述加密密钥对接收单元接收的所述加密数据流进行解密。

对应上述第四种情况，第二设备的内部结构可如图 4b 所示，包括：接收单元、中间密钥解析单元、加密密钥生成单元和解密单元。

其中，接收单元用于接收监控中心转发的来自第一设备的加密数据流，以及监控中心发送的对应第一设备数据信息的加密后的中间密钥。

中间密钥解析单元用于利用自身所在第二设备的身份密钥对接收单元接收的所述中间密钥进行解密，得到对应第一设备数据信息的中间密钥。

加密密钥生成单元用于根据中间密钥解析单元解析出的中间密钥和接收单元接收的所述加密数据流中当前加密数据包携带的随机密钥按照第三密钥生成算法生成对应该加密数据包的加密密钥。

解密单元用于利用加密密钥生成单元生成的所述加密密钥对接收单元接收的所述加密数据流中的当前加密数据包进行解密。

进一步地，第二设备中还可包括认证处理单元（图中未示出），用于对解密单元解析出的第一设备数据信息的每个原始数据单元按照第二预设规则产生认证数据，将所述认证数据与对应原始数据单元后面或前面的认证数据进行匹配，如果相匹配，则确定认证通过，表明数据是完整真实的；否则，认证不通过，数据发生错误。

具体到图 1 所示前端设备和后端设备中，如果既对前端设备发送给监控中心、监控中心发送给后端设备的监控信息进行加密保护，又对后端设备发送给监控中心、监控中心发送给前端设备的控制信息进行加密保护，则前端设备和后端设备的内部结构同时具有第一设备和第二设备的结构。

而监控中心在具体实现时，可如图 1 所示，包括：数据处理单元和安全管理单元。

其中，数据处理单元用于接收来自第一设备的加密数据流，并将该加密数据流发送给第二设备。

安全管理中心，用于存储第一设备和第二设备的身份密钥，并在第一设

备需要利用工作密钥进行加密时，为第一设备分配工作密钥，并利用第一设备的身份密钥对工作密钥加密后发送给第一设备；在第二设备接收来自第一设备的加密数据流时，利用第二设备的身份密钥对第一设备的加密密钥或中间密钥进行加密后发送给第二设备。

具体到图 1 所示的前端设备和后端设备，对于监控信息，则有：监控中心的数据处理单元，用于接收前端设备对监控信息加密后的加密数据流，根据被授权访问所述前端设备监控信息的后端设备的请求，将所述加密数据流发送给所述后端设备。

安全管理单元用于存储分别为每个前端设备和后端设备设置的唯一身份密钥，并按照第一预设规则生成工作密钥，在前端设备对自身监控信息进行编码时，利用所述前端设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给所述前端设备；在数据处理单元将前端设备的加密数据流发送给后端设备时，利用所述后端设备的身份密钥对对应所述前端设备监控信息的加密密钥或中间密钥进行加密，将加密后的加密密钥或中间密钥发送给所述后端设备。

对于控制信息，则有：数据处理单元进一步接收被授权控制设定前端设备的后端设备对控制信息加密后的加密数据流，将所述加密数据流发送给对应的前端设备。

安全管理单元进一步在后端设备需要对发送给前端设备的控制信息进行加密时，利用所述后端设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给所述后端设备；在数据处理单元将后端设备的加密数据流发送给前端设备时，利用所述前端设备的身份密钥对对应所述后端设备控制信息的加密密钥或中间密钥进行加密，将加密后的加密密钥或中间密钥发送给所述前端设备。

以上对本发明实施例中支持数据加密保护方法的监控系统进行了详细描述，下面再对本发明实施例中监控系统中数据加密保护的方法进行详细描述。图 5 为本发明实施例中监控系统中数据加密保护方法的流程示意图。如

图 5 所示，该流程包括如下步骤：

步骤 501，分别为每个第一设备设置唯一的身份密钥。

具体实现时，该身份密钥可分别存储在第一设备和监控中心中。

步骤 502，根据当前第一设备的身份密钥得到对应当前第一设备数据信息的加密密钥。

本步骤具体实现时，同样可有多种具体实现形式。对应图 1 所示系统中的四种情况，本步骤中可以是第一设备直接将自身的身份密钥作为加密密钥（一级密钥）。也可以是监控中心按照第一预设规则生成工作密钥，利用当前第一设备的身份密钥对当前生成的工作密钥进行加密，将加密后的工作密钥发送给当前第一设备，当前第一设备利用自身的身份密钥对所述加密后的工作密钥进行解密，得到所述工作密钥，将所述工作密钥作为对应的加密密钥（一级密钥）；或者，在得到所述工作密钥后，利用所述工作密钥和自身的身份密钥生成对应的加密密钥（二级密钥）；又或者，在得到所述工作密钥后，利用所述工作密钥和自身的身份密钥生成中间密钥，利用所述中间密钥与本地产生的对应每个加密数据包的随机密钥生成对应加密数据包的加密密钥（三级密钥）。

步骤 503，利用所述加密密钥对当前第一设备的数据信息进行加密，生成加密数据流。

具体加密时，可以是直接利用加密密钥对当前第一设备的原始数据信息进行加密。

或者也可以首先将当前第一设备的原始数据信息按照网络传输协议的要求封装为各个原始数据单元，然后利用加密密钥分别对每个原始数据单元中的数据载荷进行加密。

进一步地，为了同时提供数据的完整性和真实性保护，防止数据被篡改，可对数据增加认证处理，即对每个原始数据单元按照第二预设规则产生认证数据（HMAC），将认证数据附加在原始数据单元后面（或前面），再对由原始数据单元（RDU）和认证数据（HMAC）组成的数据单元加密。

对于加密密钥为三级密钥的情况，随机密钥（T-Key）还需以明文的方式随对应的加密数据包（即加密数据单元）一起传输。

步骤 504，将所述加密数据流进行传送。

具体传送时，可以将该加密数据流发送给监控中心，由监控中心对加密数据流进行解密后发送给相应的后端设备。

或者，也可以由监控中心直接将未解密的加密数据流发送给相应的后端设备。此时，可分别为每个第二设备设置唯一的身份密钥，并将该身份密钥分别存储在监控中心和对应的第二设备中。

相应地，对于步骤 502 中描述的一级密钥和二级密钥的情况，由于不涉及到第一设备的随机密钥，因此，监控中心可利用所述第二设备的身份密钥对对应所述第一设备数据信息的加密密钥进行加密，将加密后的加密密钥发送给所述第二设备。所述第二设备利用自身的身份密钥对所述加密后的加密密钥进行解密，得到所述加密密钥，利用所述加密密钥对所述第一设备的加密数据流进行解密，得到所述第一设备的数据信息。

对于步骤 502 中描述的三级密钥的情况，监控中心在将加密数据流发送给后端设备时，可利用所述第二设备的身份密钥对对应所述第一设备数据信息的中间密钥进行加密，将加密后的中间密钥发送给所述第二设备。然后该第二设备利用自身的身份密钥对所述加密后的中间密钥进行解密，得到所述中间密钥，利用所述中间密钥及所述第一设备的加密数据流中对应每个加密数据包携带的随机密钥生成对应的加密数据包的加密密钥，利用所述加密密钥对对应的加密数据包进行解密，得到所述第一设备的数据信息。

其中，如果加密数据包中存在认证数据，则得到第一设备的数据信息之后，可进一步对该数据信息进行认证处理，具体认证处理过程可以是：第二设备对第一设备数据信息的每个原始数据单元按照第二预设规则产生认证数据，将所述认证数据与对应原始数据单元后面或前面的认证数据进行匹配，如果相匹配，则确定认证通过，表明数据是完整真实的；否则，认证不通过，数据发生错误。

以上对本发明实施例中的系统及方法进行了详细描述。此外，本发明实施例中，为保证周期更新的工作密钥（W-Key）在各个设备之间的同步，即保证数据的正确加解密，除了在发送工作密钥时携带时间信息作为同步生效参考外，还可以采用如下方式。在解密端（如第二设备）缓存多组工作密钥，如三组工作密钥 W: W_{N-1}，W_N，W_{N+1}，分别对应过去、现在和将来采用的工作密钥。解密端（如第二设备）接收到加密数据后，如果用其中一个密钥解密得到的结果不对（如认证数据 HMAC 不匹配），可以先尝试用另外两个密钥解密，避免由于网络延时等原因造成的密钥更新不同步问题。

具体实现时，对应一级密钥和二级密钥的情况，可以由第二设备在得到监控中心发送的加密密钥后，进一步对所述加密密钥进行缓存，当利用当前的加密密钥对来自第一设备的加密数据流进行解密时，如果无法解开，则可进一步利用自身缓存的时间邻近的其它加密密钥对所述加密数据流进行解密。对应三级密钥的情况，则可以由第二设备在得到监控中心发送的中间密钥后，进一步对所述中间密钥进行缓存，当利用当前加密密钥对来自第一设备的加密数据流进行解密时，如果无法解开，则可进一步利用自身缓存的时间邻近的其它中间密钥及所述第一设备的加密数据流中加密数据包携带的随机密钥生成对应的加密数据包的加密密钥，利用所生成的加密密钥对对应的加密数据包进行解密。

进一步地，为了和现有技术中的第一设备的数据信息进行兼容，即使得本发明实施例中所描述的监控中心和第二设备能够处理现有技术中第一设备的数据信息，本发明实施例中的第一设备在对数据信息进行加密后，可在每个加密数据包中设置加密标志（如在数据包的包头中设置加密标志），则监控中心或第二设备在接收到来自第一设备的数据信息后，判断数据包中是否存在加密标志，如果存在，则监控中心和第二设备再执行相应的解密操作。

下面列举本发明实施例中的一个三级密钥的示例。

如图 1 所示，每个前端设备（F1,F2）和后端设备（Ba,Bb）都有唯一的身份密钥 ID。监控中心的安全管理单元（具体实现时，可以是安全中心服

务器（Security Server））维护网络内所有设备的身份密钥表和访问权限表。

安全管理单元利用前端设备 F1 的身份密钥 ID1 对当前的工作密钥 W1 加密生成 $E_{ID1}(W1)$，并发送给前端设备 F1。

前端设备 F1 用身份密钥 ID1 对接收到的 $E_{ID1}(W1)$解密，获得当前的工作密钥 W1；然后利用工作密钥 W1 和自身的身份密钥 ID1，根据密钥生成算法 F( )产生中间密钥 F(ID1,W1)，再与本地生成的随机密钥 T 按照密钥生成算法 G( )产生加密用的密钥 G(F(ID1,W1),T)；用该密钥对前端设备 F1 采集、编码的音视频数据等监控信息加密，生成加密数据流 ED1，并传回监控中心。

如果后端设备 Ba 被授权可以访问（即解码、显示、播放、存储和/或它们的组合）前端设备 F1 传回的内容，则安全管理单元利用后端设备 Ba 的身份密钥 IDa 对中间密钥 F(ID1,W1)进行加密，生成 $E_{IDa}(F(ID1,W1))$，并发送给后端设备 Ba。

后端设备 Ba 用身份密钥 IDa 对 $E_{IDa}(F(ID1,W1))$解密，获得 F(ID1,W1)；再利用随加密数据一起接收到的随机密钥 T 按照密钥生成算法 G( )产生解密用的密钥 G(F(ID1,W1),T)；用该密钥对前端设备 F1 传回的音视频数据等监控信息解密，并解码、显示、播放、存储和/或它们的组合。

后端设备 Ba 对前端设备 F1 的控制信息也采用上述方式加密，生成加密指令流 EC1，传输到前端设备 F1 后再解密并执行，此处不再详述。

其中，密钥生成算法 ***F***( )和 ***G***( )都是预设且公开的。加解密采用预共享密钥的加解密方式，不改变数据长度，兼顾安全性、实时性和实现复杂度。加密模块与解密模块是对称的，即运算逻辑完全相同。进一步的，对存储和后期离线查询检索的数据安全，还可以采用更复杂的分组加密方式。

本发明实施例中的三个密钥，身份密钥、工作密钥和随机密钥都可以根据预先定义的密钥生成规则产生加密和解密单元实际使用的密钥，且密钥的长度可选，可以采用 40-bit，64-bit，80-bit，128-bit 等，长度越大，安全性越高，运算越复杂，此处不做详述。

以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

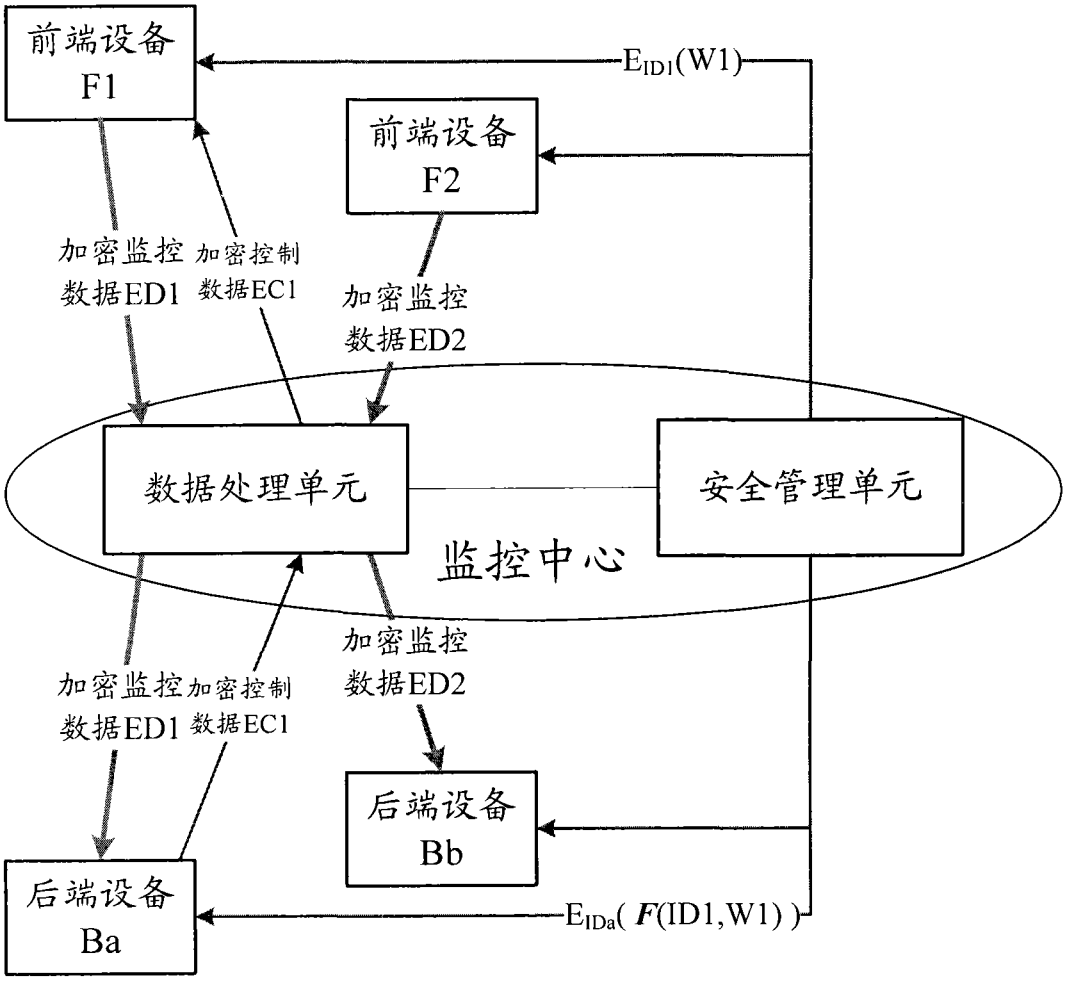

前端设备
F1
$E_{ID1}(W1)$
前端设备
F2
加密监控
数据ED1
加密控制
数据EC1
加密监控
数据ED2
数据处理单元
安全管理单元
监控中心
加密监控
数据ED2
加密监控
数据ED1
加密控制
数据EC1
后端设备
Bb
后端设备
Ba
$E_{IDa}(F(ID1,W1))$

图 1

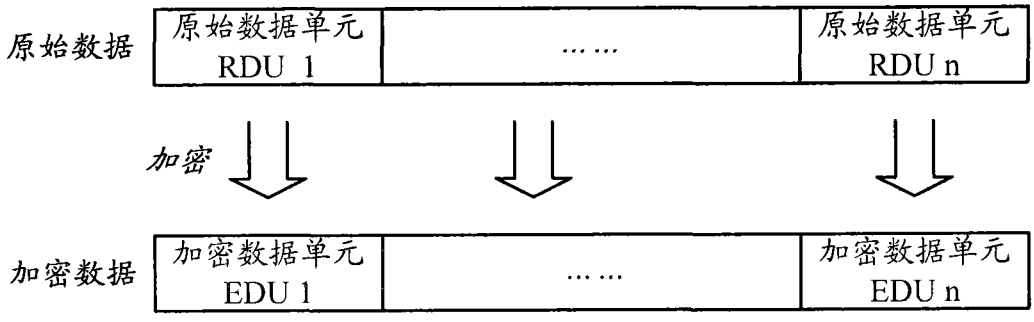

原始数据
原始数据单元
RDU 1
……
原始数据单元
RDU n
加密
加密数据
加密数据单元
EDU 1
……
加密数据单元
EDU n

图 2a

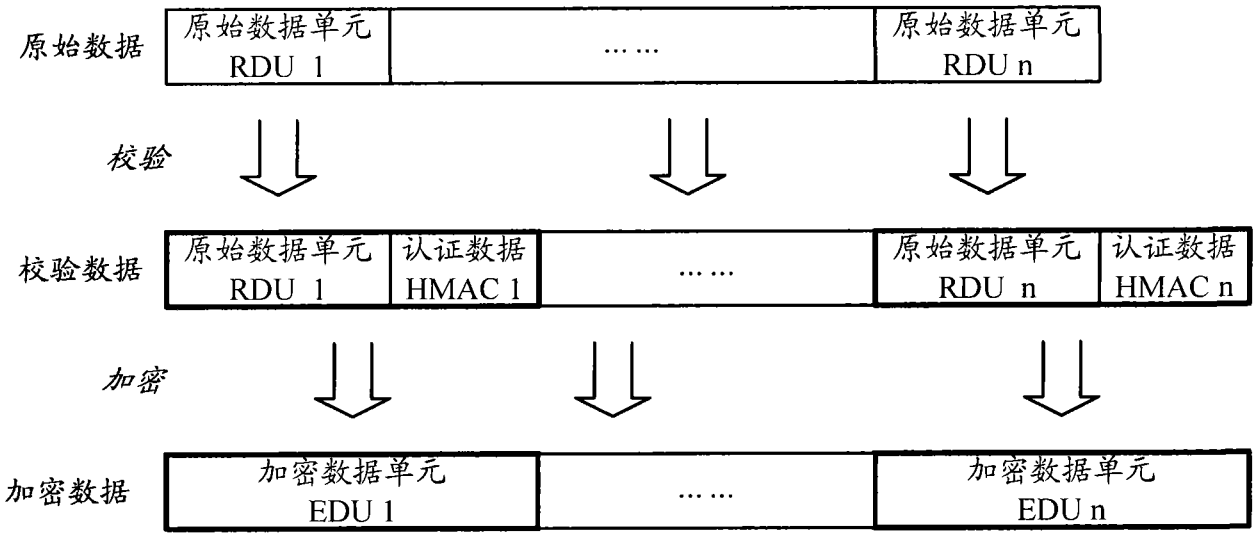

原始数据
原始数据单元 RDU 1
……
原始数据单元 RDU n
校验
校验数据
原始数据单元 RDU 1
认证数据 HMAC 1
……
原始数据单元 RDU n
认证数据 HMAC n
加密
加密数据
加密数据单元 EDU 1
……
加密数据单元 EDU n

图 2b

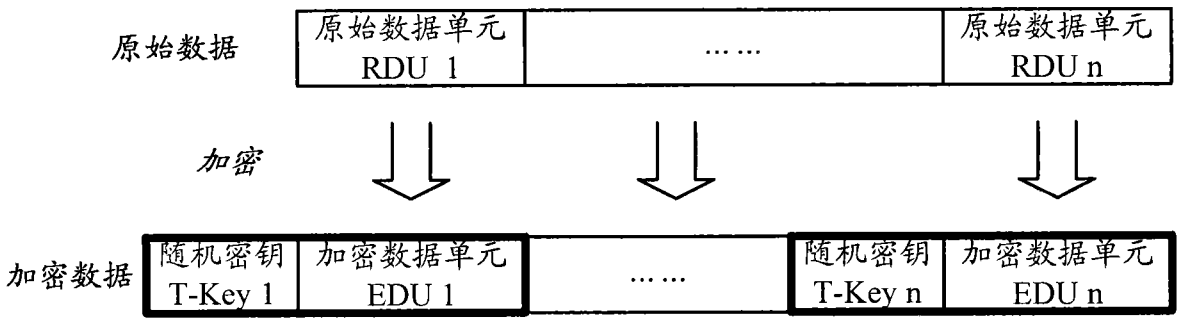

原始数据
原始数据单元 RDU 1
……
原始数据单元 RDU n
加密
加密数据
随机密钥 T-Key 1
加密数据单元 EDU 1
……
随机密钥 T-Key n
加密数据单元 EDU n

图 2c

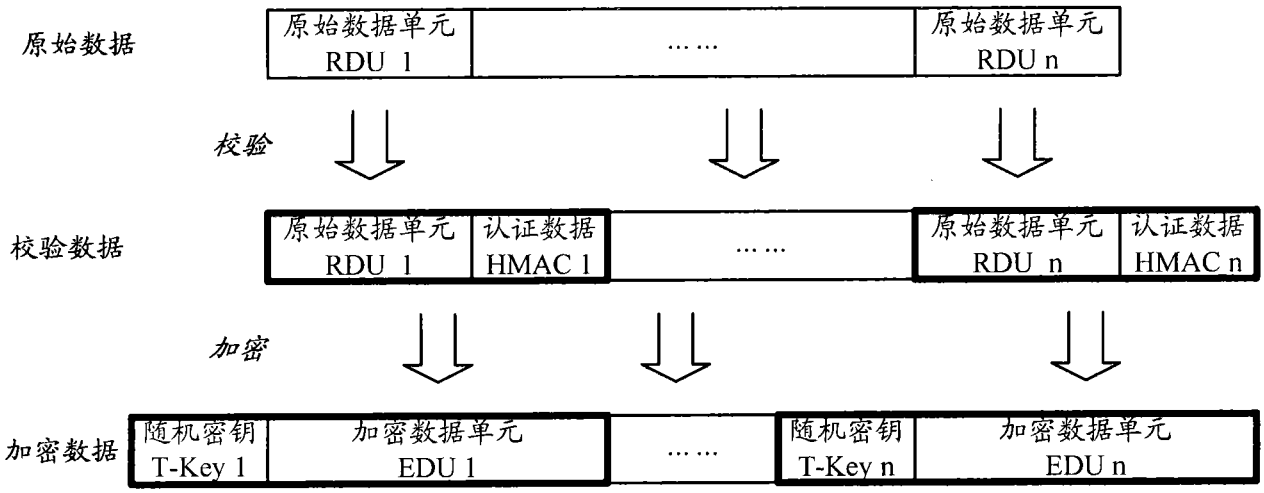

原始数据
原始数据单元 RDU 1
……
原始数据单元 RDU n
校验
校验数据
原始数据单元 RDU 1
认证数据 HMAC 1
……
原始数据单元 RDU n
认证数据 HMAC n
加密
加密数据
随机密钥 T-Key 1
加密数据单元 EDU 1
……
随机密钥 T-Key n
加密数据单元 EDU n

图 2d

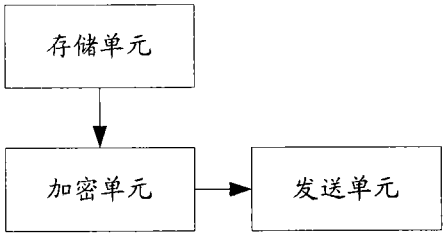

存储单元
加密单元
发送单元

图 3a

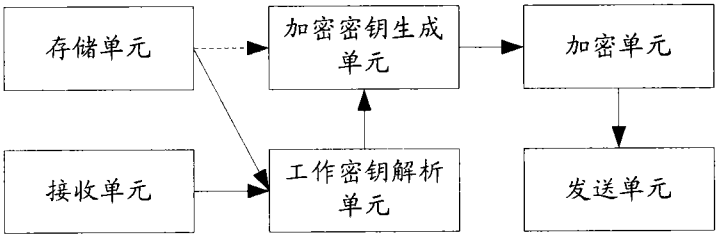

存储单元
加密密钥生成单元
加密单元
接收单元
工作密钥解析单元
发送单元

图 3b

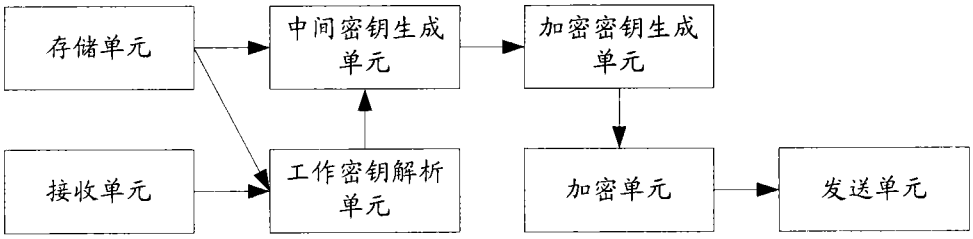

存储单元
中间密钥生成单元
加密密钥生成单元
接收单元
工作密钥解析单元
加密单元
发送单元

图 3c

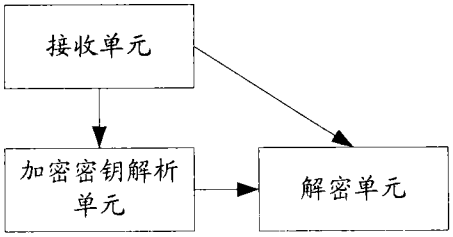

接收单元
加密密钥解析单元
解密单元

图 4a

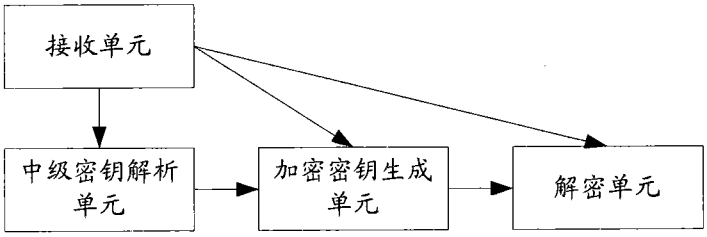

接收单元
中级密钥解析单元
加密密钥生成单元
解密单元

图 4b

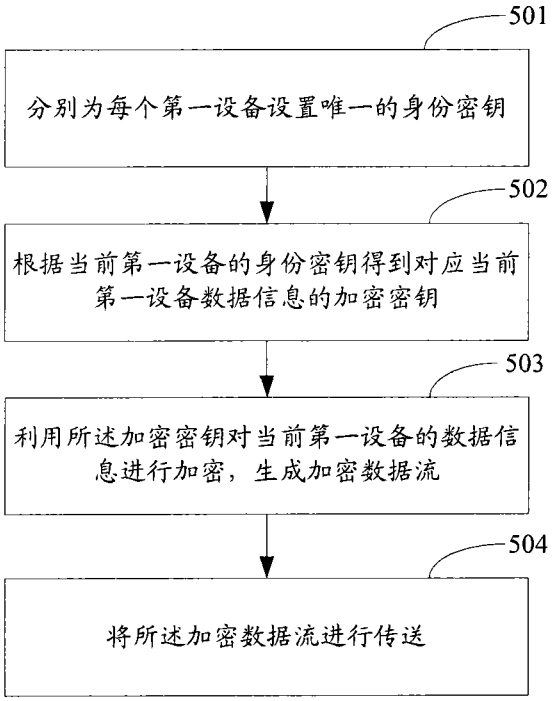

501
分别为每个第一设备设置唯一的身份密钥
502
根据当前第一设备的身份密钥得到对应当前第一设备数据信息的加密密钥
503
利用所述加密密钥对当前第一设备的数据信息进行加密，生成加密数据流
504
将所述加密数据流进行传送

图 5