(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2013 年 4 月 25 日 (25.04.2013)

WIPO | PCT

(10) 国际公布号
WO 2013/056502 A1

(51) 国际专利分类号:
H04L 9/14 (2006.01)

(21) 国际申请号: PCT/CN2011/085081

(22) 国际申请日: 2011 年 12 月 30 日 (30.12.2011)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201110317834.1 2011 年 10 月 19 日 (19.10.2011) CN

(71) 申请人 (对除美国外的所有指定国): **海尔集团公司 (HAIER GROUP CO., LTD.)** [CN/CN]; 中国山东省青岛市崂山区高科园海尔路 1 号海尔工业园, Shandong 266103 (CN)。 **海尔集团技术研发中心 (R&D CENTER OF HAIER GROUP)** [CN/CN]; 中国山东省青岛市崂山区高科园海尔路 1 号海尔工业园, Shandong 266103 (CN)。 **王袭 (WANG, Xi)** [CN/CN]; 中国山东省青岛市崂山区高科园海尔路 1 号海尔工业园, Shandong 266103 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **喻子达 (YU, Zida)** [CN/CN]; 中国山东省青岛市崂山区高科园海尔路 1 号海尔工业园海尔集团公司转交, Shandong 266103 (CN)。 **赵向阳 (ZHAO, Xiangyang)** [CN/CN]; 中国山东省青岛市崂山区高科园海尔路 1 号海尔工业园海尔集团公司转交, Shandong 266103 (CN)。 **周林 (ZHOU, Lin)** [CN/CN]; 中国山东省青岛市崂山区高科园海尔路 1 号海尔工业园海尔集团公司转交, Shandong 266103 (CN)。 **韩文 (HAN, Wen)** [CN/CN]; 中国山东省青岛市崂山区高科园海尔路 1 号海尔工业园海尔集团公司转交, Shandong 266103 (CN)。 **安娜 (AN, Na)** [CN/CN]; 中国山东省青岛市崂山区高科园海尔路 1 号海尔工业园海尔集团公司转交, Shandong 266103 (CN)。

(74) 代理人: **北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.)**; 中国北京市朝阳区西坝河西里 28 号英特公寓 C 座 104 室, Beijing 100028 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY,

[见续页]

(54) Title: HIERARCHICAL HYBRID ENCRYPTION METHOD AND APPARATUS OF SMART HOME SYSTEM

(54) 发明名称 : 一种智能家庭系统的分级混合加密方法及装置

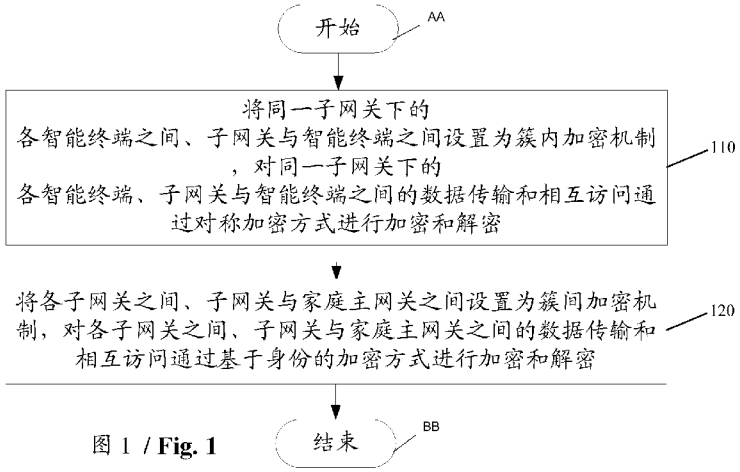

图 1 / Fig. 1

110 CONFIGURING, BETWEEN ALL SMART TERMINALS AND BETWEEN THE SUB-GATEWAYS AND SMART TERMINALS UNDER A SAME SUB-GATEWAY, AN INTRA-CLUSTER ENCRYPTION MECHANISM, AND USING SYMMETRICAL ENCRYPTION AND DECRYPTION FOR DATA TRANSMISSIONS AND FOR MUTUAL ACCESS BETWEEN SUCH SMART TERMINALS AND SUB-GATEWAYS

120 CONFIGURING, BETWEEN THE SUB-GATEWAYS AND BETWEEN THE SUB-GATEWAYS AND THE MAIN HOME GATEWAY, AN INTER-CLUSTER ENCRYPTION MECHANISM, AND USING ID-BASED ENCRYPTION AND DECRYPTION FOR DATA TRANSMISSIONS AND FOR MUTUAL ACCESS BETWEEN THE SUB-GATEWAYS AND BETWEEN THE SUB-GATEWAYS AND THE MAIN HOME GATEWAY.

AA START

BB END

(57) **Abstract**: Disclosed are a hierarchical hybrid encryption method and device for a smart home system, which comprise: configuring, between all smart terminals and between the sub-gateways and smart terminals under a same sub-gateway, an intra-cluster encryption mechanism, and using symmetrical encryption and decryption for data transmissions and for mutual access between such smart terminals and sub-gateways; configuring, between the sub-gateways and between the sub-gateways and the main home gateway, an inter-cluster encryption mechanism, and using ID-based encryption and decryption for data transmissions and for mutual access between the sub-gateways and between the sub-gateways and the main home gateway. The method of the present invention wholly satisfies the security requirements of smart home systems, taking advantage of the small overheads and fast encryption of symmetric encryption computation, and of the low deployment and running costs etc., of ID-based encryption, thus reducing installation and operational costs while ensuring security.

(57) 摘要:

[见续页]

WO 2013/056502 A1

TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) **指定国** (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明公开了一种智能家庭系统的分级混合加密方法及装置，包括：将同一子网关下的各智能终端之间、子网关与智能终端之间设置为簇内加密机制，对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过对称加密方式进行加密和解密；将各子网关之间、子网关与家庭主网关之间设置为簇间加密机制，对各子网关之间、子网关与家庭主网关之间的数据传输和相互访问通过基于身份的加密方式进行加密和解密。应用本发明，充分满足智能家庭体系的安全要求，该方法能够充分利用对称加密计算开销小，加密速度快等优点和基于身份加密部署、运行成本低等优点，在保证安全性的前提下减少了安装、运行成本。

一种智能家庭系统的分级混合加密方法及装置

技术领域

本发明涉及物联网领域，尤其涉及一种智能家庭系统的分级混合加密方法及装置。

背景技术

基于物联网的智能家庭是一个多功能网络系统，利用先进的计算机、网络通信、自动控制等先进技术，将与家庭生活相关的各种应用子系统（如安防系统、家电控制、照明控制、娱乐系统、远程监控等）有机结合，通过中央控制机或家庭网关实现集中控制。各种智能终端通过无线或有线方式与家庭网关通信，例如智能手机、笔记本等智能移动设备通过 WIFI 方式访问外部互联网；远程控制终端（如手机、PC）通过电讯网或互联网可以实现对智能家庭内部终端的远程控制。

其中保证智能家庭的数据机密性和用户数据的隐私安全是智能家居系统的重要问题。简单的访问加密策略无法满足智能家庭对安全的需求：简单的访问密码策略易于被破解、易受网络黑客攻击。恶意攻击者可以窃取或破解访问密码，实现对终端的远程控制；恶意攻击者可以伪装成合法的用户或终端设备，窃取、修改合法用户的信息和隐私数据；恶意攻击者甚至可以通过控制终端对用户造成生命的威胁（如控制天然气、安防系统等）。

传统密码体制大体上分为三类方式:

（1）“常规密码”，又称为“单钥密码”，“对称密码”。

（2）“公开钥密码”，又称为“双钥密码”，“非对称密码”。

（3）基于身份加密(IBE)。

第一种方式：在对称加密系统中，加密和解密采用相同的密钥。因为加解密密钥相同，需要通信的双方必须选择和保存他们共同的密钥，各方必须信任对方不会将密钥泄密出去，这样就可以实现数据的机密性和完整性。对称密码算法的优点是计算开销小，加密速度快，是目前用于信息加密的主要

算法。然而，对称加密系统中存在以下缺点:

（1）不适用于大型网络。对于具有 n 个用户的网络，需要 n(n-1)/2 个密钥，在用户群不是很大的情况下，对称加密系统是有效的。但是对于大型网络，当用户群很大，分布很广时，密钥的分配和保存就成了问题。

（2）密钥维护成本高。对称加密的局限性在于它存在着通信的贸易双方之间确保密钥安全交换的问题。此外，某一通信终端有几个通信关系，他就要维护几个专用密钥。

（3）它也没法鉴别通信终端发起方或通信接受方，因为的双方的密钥相同。

（4）不能用于数字签名。由于对称加密系统仅能用于对数据进行加解密处理，提供数据的机密性，因此对衬加密体制不能用于数字签名。

第二种方式：非对称加密从理论上讲，只要是用户的私有密钥没有丢失或者被窃，那么他们之间加密的信息是绝对不会被破解的。然而，由于对称加密策略本身的限制，具有以下缺点:

（1）操作繁琐。接收方必须同时准备好公共密钥和私人密钥，而发信方需要知道或者能够找出接收方的公共密钥，在大多数情况下，这意味着发信方必须搜寻出一个证书认证以检索到目标接收方的公共密钥。并且，只有在接收方确定使用该加密方法并拥有可用的密钥的情况下，才能进行公钥加密，而大多数人都没有公共密钥。

（2）加密速度非常缓慢。由于要进行大量的数学运算，即使加密少量的信息也需要花费大量的时间。

第三种方式：与传统公钥加密相比，基于身份的加密不需要任何证书，接收方的公共密钥源自他的身份信息。IBE 所需要的基础设施比传统加密方法简单得多，这意味这更少的服务器和更简便的安装。IBE 加密的运行费用仅为那些公钥系统的五分之一，并且 IBE 用户的生产率比那些公共密钥用户高五倍。密钥设有使用期限，因此不需要予以撤销。在传统公钥系统中，密钥必须予以撤销。能够延迟信息解密以便于以后的解密。由于引入了第三方服务器，IBE 加密有以下缺点:

（1）需要一个集中服务器，这也增大了泄漏的安全风险，另外 IBE 的集中管理方式暗示着有些密钥必须以代管的形式创建和保存。

（2）在发信方或者接收方和IBE服务器间需要一个安全通道来传送私钥。

综上所述，现有的加密技术无论对称加密、公钥加密还是基于身份的加密，都有各自的缺点，适应于单一的应用场景。然而对于功能复杂、多种网络融合的智能家庭系统，单一的加密机制无法满足安全需求。因此当前需要一种针对智能家庭特点设计的加密体系的技术方案。

发明内容

本发明所要解决的技术问题是提供一种智能家庭系统的分级混合加密方法及装置，解决了当前单一的加密机制不能满足智能家庭系统安全需求的问题。

为了解决上述问题，本发明提供了一种智能家庭系统的分级混合加密方法，包括:

将同一子网关下的各智能终端之间、子网关与智能终端之间设置为簇内加密机制，对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过对称加密方式进行加密和解密;

将各子网关之间、子网关与家庭主网关之间设置为簇间加密机制，对各子网关之间、子网关与家庭主网关之间的数据传输和相互访问通过基于身份的加密方式进行加密和解密。

进一步地，上述方法还可包括: 所述对称加密方式包括 DES 算法的对称加密方式、3DES 算法的对称加密方式、TDEA 算法的对称加密方式、Blowfish 算法的对称加密方式、RC5 算法的对称加密方式或 IDEA 算法的对称加密方式。

进一步地，上述方法还可包括: 所述对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过对称加密方式进行加密和解密的步骤，包括:

对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过RC5算法的对称加密方式进行加密和解密，其中，RC5算法通过分组大小参数、密钥大小参数和加密轮数参数进行调整，使用异或、加和循环的运算方式进行运算。

进一步地，上述方法还可包括：所述对各子网关之间、子网关与家庭主网关之间的数据传输和相互访问通过基于身份的加密方式进行加密和解密的步骤，包括：

初始化系统，输入所需安全参数，得到系统参数和主密钥信息；

根据用户的身份信息，生成用户对应的私钥信息；

通过用户的身份信息作为公钥信息，对需要加密的明文进行加密，得到对应的密文；通过用户的身份信息相对应的私钥信息，对密文进行解密，得到对应的明文。

进一步地，上述方法还可包括：所述基于身份的加密方式包括：非交互式密钥更新的基于身份加密方式或Waters IBE方式。

本发明还提供了一种智能家庭系统的分级混合加密装置，包括：加密分级单元，对称加密单元和基于身份的加密单元，其中，

所述加密分级单元，用于将同一子网关下的各智能终端之间、子网关与智能终端之间设置为簇内加密机制，将各子网关之间、子网关与家庭主网关之间设置为簇间加密机制；

所述对称加密单元，用于对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过对称加密方式进行加密和解密；

所述基于身份的加密单元，用于对各子网关之间、子网关与家庭主网关之间的数据传输和相互访问通过基于身份的加密方式进行加密和解密。

进一步地，上述装置还可包括：所述对称加密单元采用的所述对称加密方式包括DES算法的对称加密方式、3DES算法的对称加密方式、TDEA算法的对称加密方式、Blowfish算法的对称加密方式、RC5算法的对称加密方式或IDEA算法的对称加密方式。

进一步地，上述装置还可包括：所述对称加密单元对同一子网关下的各

智能终端、子网关与智能终端之间的数据传输和相互访问通过对称加密方式进行加密和解密，是指:

对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过 RC5 算法的对称加密方式进行加密和解密，其中，RC5 算法通过分组大小参数、密钥大小参数和加密轮数参数进行调整，使用异或、加和循环的运算方式进行运算。

进一步地，上述装置还可包括：所述基于身份的加密单元对各子网关之间、子网关与家庭主网关之间的数据传输和相互访问通过基于身份的加密方式进行加密和解密，是指:

所述基于身份的加密单元进行初始化，输入所需安全参数，得到系统参数和主密钥信息；根据用户的身份信息，生成用户对应的私钥信息；通过用户的身份信息作为公钥信息，对需要加密的明文进行加密，得到对应的密文；通过用户的身份信息相对应的私钥信息，对密文进行解密，得到对应的明文。

进一步地，上述装置还可包括：所述基于身份的加密单元采用的所述基于身份的加密方式包括：非交互式密钥更新的基于身份加密方式或 Waters IBE 方式。

与现有技术相比，应用本发明，充分满足智能家庭体系的安全要求，该方法能够充分利用对称加密计算开销小，加密速度快等优点和基于身份加密部署、运行成本低等优点，在保证安全性的前提下减少了安装、运行成本。

附图说明

图 1 是本发明的智能家庭系统的分级混合加密方法的流程图;

图 2 是本发明的智能家庭系统的分级混合加密装置的结构示意图。

具体实施方式

本发明的智能家庭的分级混合加密方法，适用于分级结构的智能家庭体系，主要构思在于：该加密方法分为簇内加密机制和簇间加密机制两个等级：各智能终端之间和子网关与智能终端之间为簇内加密级，采用对称加密机

制；各子网关之间和子网关与家庭主网关之间为簇间加密级，采用基于身份的加密机制。

下面结合附图和具体实施方式对本发明作进一步说明。

如图 1 所示，本发明的一种智能家庭系统的分级混合加密方法，包括:

步骤 110、将同一子网关下的各智能终端之间、子网关与智能终端之间设置为簇内加密机制，对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过对称加密方式进行加密和解密;

步骤 120、将各子网关之间、子网关与家庭主网关之间设置为簇间加密机制，对各子网关之间、子网关与家庭主网关之间的数据传输和相互访问通过基于身份的加密方式进行加密和解密。

第一部分：簇内加密机制:

簇内加密负责对同一子网关下的智能终端间、智能终端与子网关间的数据进行加密，本发明采用对称加密方式，对称加密是一种采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密，这种加密方法称为对称加密，也称为单密钥加密。由于其速度快，对称性加密通常在消息发送方需要加密大量数据时使用。

对称加密算法包括 DES 算法、3DES 算法、TDEA 算法、Blowfish 算法、RC5 算法或 IDEA 算法等，本发明对此不作限定。

其中，本发明可采用 RC5 加密算法，RC5 加密算法适用于不同字长的微处理器，可移植性好；六轮以上时即可抗线性攻击；通过调整字长、密钥长度和迭代轮数可以在安全性和速度上取得折中

RC5 分组密码算法是参数可变的分组密码算法，三个可变的参数是：分组大小、密钥大小和加密轮数。在此算法中使用了三种运算：异或、加和循环。RC5 加密解密的处理过程如下:

（1）创建密钥组

RC5 算法加密时使用了 2r+2 个密钥相关的 32 位字，这里 r 表示加密的轮数。创建这个密钥组的过程是非常复杂的但也是直接的，首先将密钥字节拷贝到 32 位字的数组 L 中，如果需要，最后一个字可以用零填充。然后利用线性同余发生器模 2 初始化数组 S:

对于 i=1 到 2(r+1)-1 ;

其中对于 16 位字 32 位分组的 RC5，P=0xb7e1, Q=0x9e37 ;

对于 32 位字和 64 位分组的 RC5，P=0xb7e15163, Q=0x9e3779b9 ;

对于 64 位字和 128 位分组，

P=0xb7151628aed2a6b ,Q=0x9e3779b97f4a7c15 ;

最后将 L 与 S 混合，混合过程如下:

i=j=0

A=B=0

处理 3n 次（这里 n 是 2(r+1)和 c 中的最大值，其中 c 表示输入的密钥字的个数）

（2）加密处理

在创建完密钥组后开始进行对明文的加密，加密时，首先将明文分组划分为两个 32 位字: A 和 B（在假设处理器字节顺序是 little-endian、w=32 的情况下，第一个明文字节进入 A 的最低字节，第四个明文字节进入 A 的最高字节，第五个明文字节进入 B 的最低字节，以此类推），其中操作符<<<表示循环左移，加运算是模。

输出的密文是在寄存器 A 和 B 中的内容

（3）解密处理

解密也是很容易的，把密文分组划分为两个字: A 和 B（存储方式和加密一样），这里符合>>>是循环右移，减运算也是模。

RC5 的程序实现包括以下几部分：主函数、循环左移和右移函数、产生子密钥的函数、产生初试密钥的函数、取最近奇数的函数、加密函数、解密函数。

第二部分：簇间加密机制

簇间加密负责对子网关间、子网关与主网关间的数据进行加密。

簇间加密选择和改进现有的基于身份的加密算法，设计适用于智能家居系统的基于身份的加密方案。

其中，基于身份的加密方案包括：非交互式密钥更新的基于身份加密方式（IBE－NIKU）或 Waters IBE 方式等。

其中，本发明的基于身份的加密方案设计包括四部分：系统初始化参数生成算法、私钥生成算法、加密算法、解密算法。

（a）系统初始化参数生成算法。系统初始化参数生成算法主要是生成建立系统所需的公开系统参数和秘密系统参数。该算法输入是安全参数，输出是系统参数和主密钥。

（b）私钥生成算法。根据用户的身份信息，生成用户对应的私钥。

（c）加密算法。利用用户的身份信息作为公钥，对需要加密的明文进行加密，得到对应的密文。

（d）解密算法。利用用户的身份信息相对应的私钥，对密文进行解密，得到对应的明文。

本发明采用基于身份的加密机制，具体采用 Waters IBE 方式，该加密机制包括以下几个步骤：

（1）系统参数生成。用户身份信息是长度为 n 的比特串，随机选取一个正整数 q，选取两个 p 阶群 G 和 G_1，选取双线性映射 $\hat{e}: G \times G \rightarrow G_1$，PKG 随机选择 G 的生成元 $g \in G$，随机选择 $\partial \in Z_q$，假定 $g_1 = g^{\partial}$；随机选择

$g_2 \in G$，$ú \in G$,向量$U = (u_1, u_2, u_3, u_4 \cdots u_n) \in G^n$。系统参数和主密钥为：

$\pi = \{g, g_1, g_2, ú, U\}, msk = g_2^{\partial}$;

(2)私钥生成。已知γ是一个身份信息，γ_i表示γ的第 i 位，并且$V \subseteq \{1,2,314, \cdots n\}$是所有$\gamma_i = 1$的 i 的集合，随机选择$r \in Z_q$，则身份$\gamma$的私钥为：

$$d_\gamma = \left(g_2^{\partial} \left(ú \prod_{i \in \gamma} u_i \right)^r, g^r \right);$$

（3）加密。已知明文$M \in G_1$和身份γ。随机选择$t \in Z_q$,则以身份γ加密后的密文为：

$$C = \left(\hat{e}(g_1, g_2)^t M, g^t, \left(ú \prod_{i \in \gamma} u_i \right)^t \right);$$

(4)解密。已知密文$C = (C_1, C_2, C_3)$是消息 M 在身份γ下的加密密文，则密文 C 以私钥$d_\gamma = (d_1, d_2)$解密，解密后的明文为

$$M = C_1[\hat{e}(d_2, C_3)/\hat{e}(d_1, C_2)]。$$

如图 2 所示，本发明还提供了一种智能家庭系统的分级混合加密装置，包括：加密分级单元 201，对称加密单元 202 和基于身份的加密单元 203，其中，

所述加密分级单元 201，用于将同一子网关下的各智能终端之间、子网关与智能终端之间设置为簇内加密机制，将各子网关之间、子网关与家庭主网关之间设置为簇间加密机制；

所述对称加密单元 202，用于对同一子网关下的各智能终端、子网关与

智能终端之间的数据传输和相互访问通过对称加密方式进行加密和解密;

所述基于身份的加密单元 203，用于对各子网关之间、子网关与家庭主网关之间的数据传输和相互访问通过基于身份的加密方式进行加密和解密。

所述对称加密单元202采用的所述对称加密方式包括DES算法的对称加密方式、3DES 算法的对称加密方式、TDEA 算法的对称加密方式、Blowfish 算法的对称加密方式、RC5 算法的对称加密方式或 IDEA 算法的对称加密方式。

所述对称加密单元 202 对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过对称加密方式进行加密和解密，是指:

对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过 RC5 算法的对称加密方式进行加密和解密，其中，RC5 算法通过分组大小参数、密钥大小参数和加密轮数参数进行调整，使用异或、加和循环的运算方式进行运算。

所述基于身份的加密单元 203 对各子网关之间、子网关与家庭主网关之间的数据传输和相互访问通过基于身份的加密方式进行加密和解密，是指:

所述基于身份的加密单元 203 进行初始化，输入所需安全参数，得到系统参数和主密钥信息；根据用户的身份信息，生成用户对应的私钥信息；通过用户的身份信息作为公钥信息，对需要加密的明文进行加密，得到对应的密文；通过用户的身份信息相对应的私钥信息，对密文进行解密，得到对应的明文。

所述基于身份的加密单元 203 采用的所述基于身份的加密方式包括：非交互式密钥更新的基于身份加密方式或 Waters IBE 方式。

本发明的一种智能家庭分级混合加密的方案，该方案主要有以下关键点:

（1）将加密、解密技术应用到智能家庭体系中，满足了智能家庭的安

全要求，解决了存在的安全隐患。

（2）针对智能家庭的独特的体系结构，采用分级、混合加密解密策略。

（3）充分利用对称加密速度快，多用于大量数据加密的环境的优点和基于身份的部署、运行成本低的优点，在保证安全性的前提下减少了安装、运行成本。

以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉该技术的人在本发明所揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

权 利 要 求 书

1、 一种智能家庭系统的分级混合加密方法，其特征在于，包括:

将同一子网关下的各智能终端之间、子网关与智能终端之间设置为簇内加密机制，对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过对称加密方式进行加密和解密;

将各子网关之间、子网关与家庭主网关之间设置为簇间加密机制，对各子网关之间、子网关与家庭主网关之间的数据传输和相互访问通过基于身份的加密方式进行加密和解密。

2、 如权利要求 1 所述的方法，其特征在于，

所述对称加密方式包括 DES 算法的对称加密方式、3DES 算法的对称加密方式、TDEA 算法的对称加密方式、Blowfish 算法的对称加密方式、RC5 算法的对称加密方式或 IDEA 算法的对称加密方式。

3、 如权利要求 2 所述的方法，其特征在于，

所述对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过对称加密方式进行加密和解密的步骤，包括:

对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过 RC5 算法的对称加密方式进行加密和解密，其中，RC5 算法通过分组大小参数、密钥大小参数和加密轮数参数进行调整，使用异或、加和循环的运算方式进行运算。

4、 如权利要求 1 所述的方法，其特征在于，

所述对各子网关之间、子网关与家庭主网关之间的数据传输和相互访问通过基于身份的加密方式进行加密和解密的步骤，包括:

初始化系统，输入所需安全参数，得到系统参数和主密钥信息;

根据用户的身份信息，生成用户对应的私钥信息;

通过用户的身份信息作为公钥信息，对需要加密的明文进行加密，得到对应的密文; 通过用户的身份信息相对应的私钥信息，对密文进行解密，得到对应的明文。

5、 如权利要求 1 或 4 所述的方法，其特征在于，

所述基于身份的加密方式包括：非交互式密钥更新的基于身份加密方式或 Waters IBE 方式。

6、 一种智能家庭系统的分级混合加密装置，其特征在于，

包括：加密分级单元，对称加密单元和基于身份的加密单元，其中，

所述加密分级单元，用于将同一子网关下的各智能终端之间、子网关与智能终端之间设置为簇内加密机制，将各子网关之间、子网关与家庭主网关之间设置为簇间加密机制；

所述对称加密单元，用于对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过对称加密方式进行加密和解密；

所述基于身份的加密单元，用于对各子网关之间、子网关与家庭主网关之间的数据传输和相互访问通过基于身份的加密方式进行加密和解密。

7、 如权利要求 6 所述的装置，其特征在于，

所述对称加密单元采用的所述对称加密方式包括 DES 算法的对称加密方式、3DES 算法的对称加密方式、TDEA 算法的对称加密方式、Blowfish 算法的对称加密方式、RC5 算法的对称加密方式或 IDEA 算法的对称加密方式。

8、 如权利要求 7 所述的装置，其特征在于，

所述对称加密单元对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过对称加密方式进行加密和解密，是指：

对同一子网关下的各智能终端、子网关与智能终端之间的数据传输和相互访问通过 RC5 算法的对称加密方式进行加密和解密，其中，RC5 算法通过分组大小参数、密钥大小参数和加密轮数参数进行调整，使用异或、加和循环的运算方式进行运算。

9、 如权利要求 6 所述的装置，其特征在于，

所述基于身份的加密单元对各子网关之间、子网关与家庭主网关之间的数据传输和相互访问通过基于身份的加密方式进行加密和解密，是指：

所述基于身份的加密单元进行初始化，输入所需安全参数，得到系统参数和主密钥信息；根据用户的身份信息，生成用户对应的私钥信息；通过用户的身份信息作为公钥信息，对需要加密的明文进行加密，得到对应的密文；通过用户的身份信息相对应的私钥信息，对密文进行解密，得到对应的明文。

10、 如权利要求 6 或 9 所述的装置，其特征在于，

所述基于身份的加密单元采用的所述基于身份的加密方式包括：非交互式密钥更新的基于身份加密方式或 Waters IBE 方式。

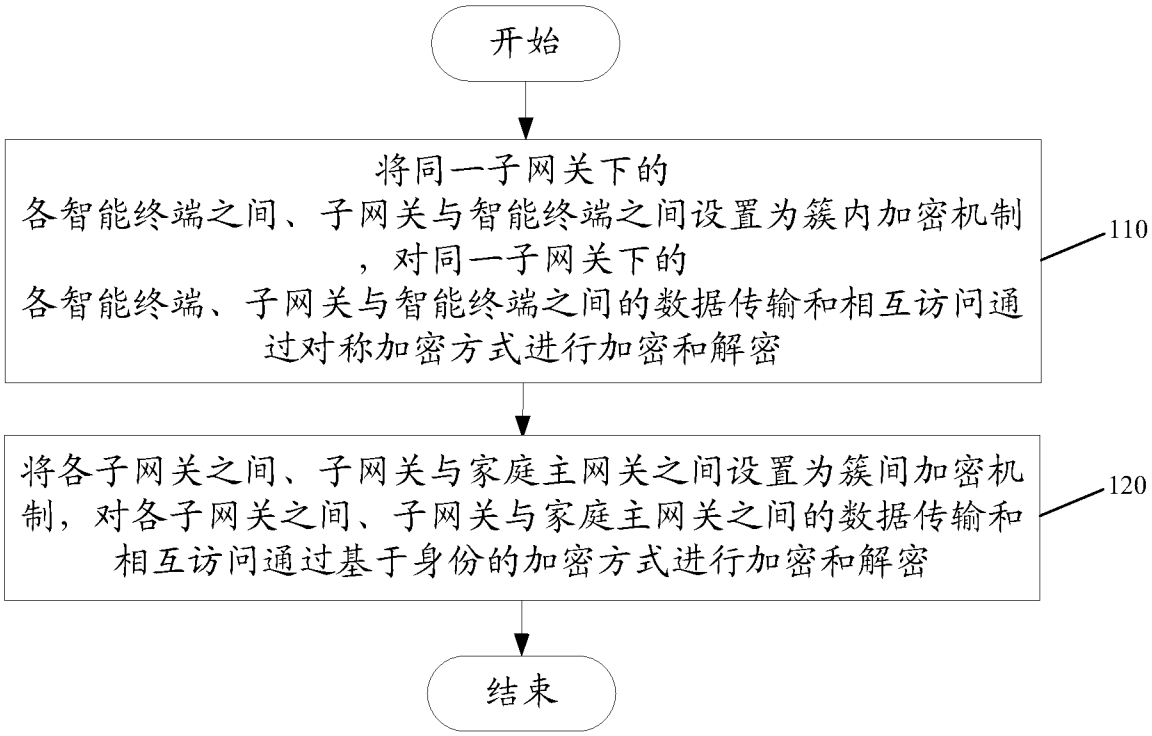
开始
将同一子网关下的
各智能终端之间、子网关与智能终端之间设置为簇内加密机制，对同一子网关下的
各智能终端、子网关与智能终端之间的数据传输和相互访问通过对称加密方式进行加密和解密
110
将各子网关之间、子网关与家庭主网关之间设置为簇间加密机制，对各子网关之间、子网关与家庭主网关之间的数据传输和相互访问通过基于身份的加密方式进行加密和解密
120
结束

图 1

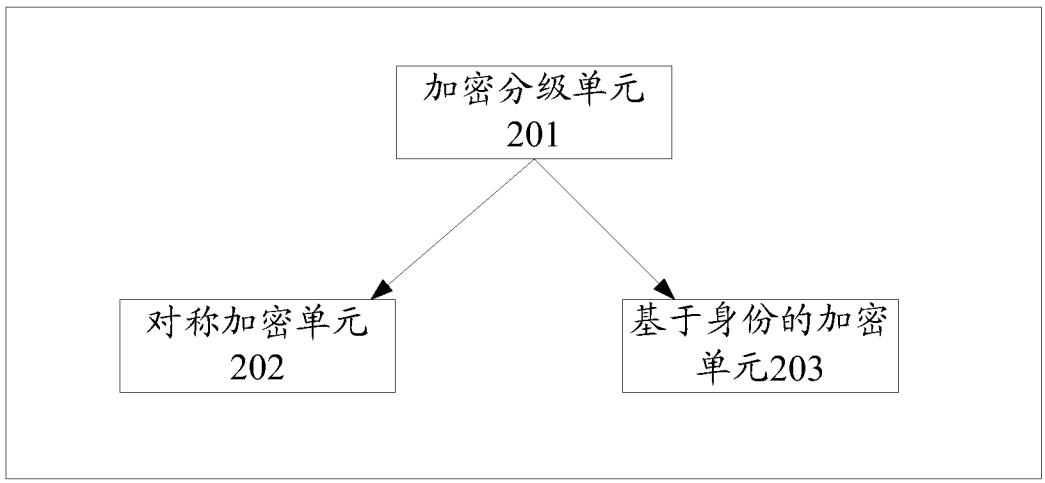
加密分级单元
201
对称加密单元
202
基于身份的加密
单元203

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/085081

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/14 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04W, H04L, H04B, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, CNTXT: Internet of things, home, network, symmetr+, encrypt+, ID, identity, sub+, IBE, hybrid

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 1917422 A (BEIJING INSTITUTE OF TECHNOLOGY), 21 February 2007 (21.02.2007), description, page 2, 4th to last paragraph to page 3, paragraph 4, and figure 1	1-3, 6-8
Y		4-5, 9-10
Y	CN 101743715 A (SAMSUNG ELECTRONICS CO., LTD.), 16 June 2010 (16.06.2010), description, paragraphs 0032-0034	4-5, 9-10
A	CN 1479483 A (LENOVO (BEIJING) CO., LTD.), 03 March 2004 (03.03.2004), the whole document	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 June 2012 (28.06.2012)	**02 August 2012 (02.08.2012)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **XU, Hongyan** Telephone No.: (86-10) **62413605**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2011/085081

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1917422 A	21.02.2007	None	
CN 101743715 A	16.06.2010	WO 2009025459 A2	26.02.2009
		KR 20090019228 A	25.02.2009
		RU 2437229 C2	20.12.2011
		US 2009055648 A1	26.02.2009
		EP 2181521 A2	05.05.2010
		JP 2010537541 A	02.12.2010
CN 1479483 A	03.03.2004	None	

国际检索报告

国际申请号
PCT/CN2011/085081

A. 主题的分类

H04L9/14 (2006.01) i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04W,H04L,H04B,H04Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT,WPI,EPODOC,CNTXT:家庭，物联网，加密，对称，身份，子，混合,home,network,symmetr+,encrypt+,ID,identity,sub+,IBE,hybrid

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN1917422A(北京理工大学)21.2 月 2007(21.02.2007) 说明书第 2 页倒数第 4 段-第 3 页第 4 段、附图 1	1-3,6-8
Y		4-5,9-10
Y	CN101743715A(三星电子株式会社)16.6 月 2010(16.06.2010) 说明书第 0032 段-0034 段	4-5,9-10
A	CN1479483A(联想(北京)有限公司)03.3 月 2004(03.03.2004)全文	1-10

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
28.6 月 2012(28.06.2012)	**02.8 月 2012 (02.08.2012)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 许洪岩 电话号码：(86-10) **62413605**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2011/085081

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1917422A	21.02.2007	无	
CN101743715A	16.06.2010	WO2009025459A2	26.02.2009
		KR20090019228A	25.02.2009
		RU2437229C2	20.12.2011
		US2009055648A1	26.02.2009
		EP2181521A2	05.05.2010
		JP2010537541A	02.12.2010
CN1479483A	03.03.2004	无	