研究与开发

基于 ECC 的智能家居密钥管理机制的实现

程文彬[1]，刘佳[2]

（1. 电子科技大学中山学院，广东 中山 528400;
2. 电子科技大学机械电子工程学院，四川 成都 611731）

摘　要：目前智能家居系统的数据加密技术多采用对称加密方式，但是这种方式存在密钥管理的问题，为实现密钥的安全，智能家居系统采用非对称加密技术，在此基础上设计了基于椭圆曲线密码体制（ECC）的密钥管理机制来达到保障密钥安全的目的。本密钥管理机制包括基于 ECC 的数据加密密钥管理机制和基于 ECC 的数字签名密钥管理机制，它们可以使得无线网络节点在身份认证，密钥的产生、分发、存储、更新等环节中密钥的安全性得到保障，其中密钥的存储环节利用了芯片内部闪存的读保护机制，实现了硬件级别的安全存储。最后对本机制的安全性、耗时和可扩展性进行了分析，结果表明该机制具有较强的安全性和可扩展性，在耗时方面优于 E-G 密钥管理方案。

关键词：智能家居；密钥管理；椭圆曲线密码体制；数字签名

中图分类号：TP393　　**文献标识码**：A

doi: 10.11959/j.issn.1000−0801.2017195

Realization of smart home key management mechanism based on ECC

CHENG Wenbin[1], LIU Jia[2]

1. Zhongshan Institute, University of Electronic Science and Technology of China, Zhongshan 528400, China
2. School of Mechatronics Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

Abstract: At present, the data encryption technology of smart home system uses symmetric encryption method, but there is a problem with key management in this way. To achieve the security of the key, the smart home system uses asymmetric encryption technology. On this basis, the key management mechanism based on ECC was designed to achieve the purpose of guaranteeing key security. The key management mechanism includes an ECC-based data encryption key management mechanism and an ECC-based digital signature key management mechanism. So that the wireless network node in the identity authentication, the key generation, distribution, storage, update and other aspects of the key security were guaranteed. Finally, the security, time-consuming and scalability of this mechanism were analyzed. The results show that the mechanism has strong security and expansibility, and it is superior to E-G key management scheme in time-consuming.

Key words: smart home, key management, elliptic curve cryptography mechanism, digital signature

收稿日期：2017−03−24；修回日期：2017−06−07

1 引言

随着无线通信技术的普及，智能家居[1]逐渐进入寻常百姓家，随之带来的安全问题也逐渐被重视。智能家居家庭内部网络采用的是无线射频通信，鉴于射频信号的开放性，只要在射频通信范围内，任何人均可接收该信号，这就给智能家居系统的使用者带来了很大的安全隐患。鉴于智能家居家庭内部无线网络面临的威胁，需要为该无线网络设计一套能适用于智能家居环境的安全防护机制，以保障该网络的通信安全。

无线网络的通信安全分为通信内容的安全以及通信网络服务的可靠性和可用性。通信内容的安全主要包括：通信数据的保密性，防窃听；通信数据的完整性，防篡改；通信数据的真实性，防伪造；通信数据的新鲜性，防重放。

为保障通信内容的安全，需要设计数据加密算法和数字签名算法，根据柯克霍夫原则，密码系统的安全性由密钥的保密性决定，而不是算法的保密性，密码系统密钥的安全十分重要。本文的智能家居家庭内部网络采用的是基于椭圆曲线密码（elliptic curve cryptography，ECC）体制[2]的数据加密算法和数字签名算法，并设计了一套针对该加密算法和数字签名的密钥管理机制[3]，保障加密算法和数字签名算法密钥的安全性，从而保障智能家居家庭内部无线网络通信内容的安全。

目前，密钥管理的主要研究方向有基于密钥分配中心的密钥管理方案、随机密钥预分配机制、非对称密钥管理机制等。本文采用的基于椭圆曲线的数据加密算法和数字签名算法属于非对称密码体制[4]，相比于对称密码体制，非对称密码体制在密钥管理方面有着天然的优势，比如密钥的分配、更新、网络扩展方面等，因此非对称密码体制密钥的安全性更高[5]。随机密钥预分配机制耗时较长，而基于密钥分配中心的密钥管理方案则需要一个只服务于保密功能的中心，该中心增加了无线网络系统的硬件成本，因此本文采用的是基于非对称密码体制的密钥管理来设计适用于智能家居家庭内部无线网络的密钥管理机制。

本文选用 STM32F407 芯片作为智能家居系统中智能网关的主控芯片，选用 STM32F103 芯片作为路由节点和家电终端节点的主控芯片，选用 CC1101 射频芯片作为通信模块的主控芯片。智能网关以及其他节点通过 433 MHz 的射频信号，构成以智能网关为根节点的树型无线通信网络。各个节点在组网过程中需要向智能网关表明自己的身份，智能网关验证通过后才能加入网络，网络组建完成后，节点间的通信内容将会被加密，保证通信内容的保密性；同时内容信息会被节点进行数字签名，保证内容信息的完整性、不可否认性和不可抵赖性；数据加密密钥会被定期更新，防止被攻击者长期监听获得足够的密文进行破解；密钥在使用期间的存储使用了硬件级的安全存储技术，保证了密钥的安全存储；组网完成后，如果有新节点加入，加入过程也非常便捷，保证了可扩展性。本文设计密钥管理机制的目的就是对上述过程中的密钥进行全程的安全管理，从而保障智能家居家庭内部无线网络通信内容的安全。

本文设计的密钥管理机制充分利用了 STM32 全球唯一的芯片 ID，将芯片 ID 作为节点的身份信息。在密钥存储环节，利用 STM32 芯片的片内 flash（闪存）的读保护功能，实现了硬件级别的密钥安全存储。对于数据加密算法的密钥产生环节，密钥由各节点自己产生，该方式的安全性优于密钥由中心产生然后分发的方式。本文将密钥设计为与时间有关的值，定期更新密钥，这样密钥的安全性得到了进一步的保障。

2 智能家居系统框架

智能家居系统硬件结构如图 1 所示，智能家

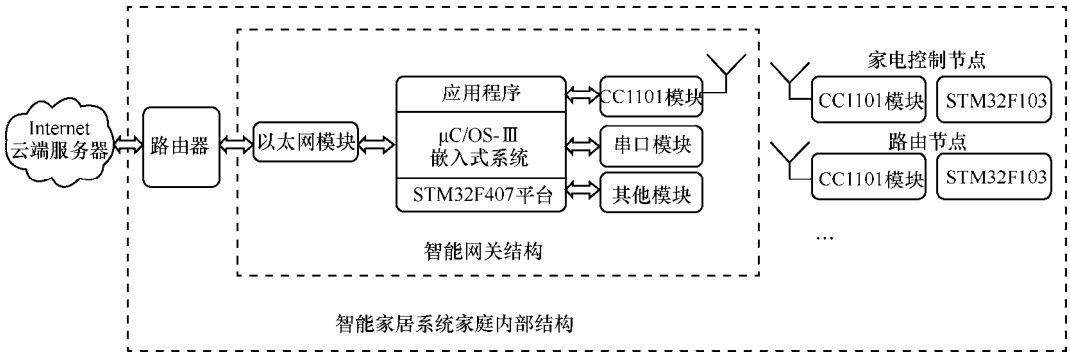

图 1　智能家居系统硬件结构

居中的核心节点是智能网关，智能网关以 STM32F407 芯片为核心硬件平台，芯片外接的模块有 CC1101 射频通信模块、串口模块、以太网模块以及其他模块。CC1101 模块实现家庭内部与其他节点之间的无线通信，串口模块实现智能网关的程序下载和调试，而以太网模块则实现智能网关与路由器之间的通信，便于将智能家居系统家庭内部网络接入互联网，实现将家庭数据上传云端以及对智能家居系统的远程控制。智能网关管理着智能家居系统内部的很多资源，因此在智能网关中移植嵌入式操作系统 μC/OS-Ⅲ，对系统资源进行调度和管理，可以实现系统资源的最大化利用，并在其上设计应用程序，实现相应的应用功能，比如 CC1101 模块的的无线通信功能等。

为实现智能家居的集中无线控制，设计了家电控制节点，该节点由 CC1101 模块和主控芯片 STM32F103 等组成，CC1101 模块负责实现无线通信，STM32F103 芯片则负责利用 CC1101 模块实现与智能网关之间的无线通信，接收和解析用户利用手机或者 PC 端发送的控制指令，经 Internet、智能网关后发送给家电控制节点，从而实现家电设备的控制，同时也能将家电设备的相关信息发送给智能网关，然后由智能网关上传云端。

智能家居家电控制节点可能处于某些通信不方便的位置，由于 CC1101 通信模块的通信距离的限制导致不能直接和智能网关通信，需要路由节点来做路由和中继，因此设计了路由节点来做通信转发。路由节点的硬件结构由 CC1101 模块进行无线通信，由 STM32F103 作主控芯片。

各个节点安装完成上电后，向外发射射频信号，进行组网，智能家居家庭内部无线网络拓扑结构如图 2 所示。以智能网关为根节点，路由节点完成路由功能，家电控制节点作为终端节点，组成树型的网络拓扑，家电控制节点之间不进行通信。

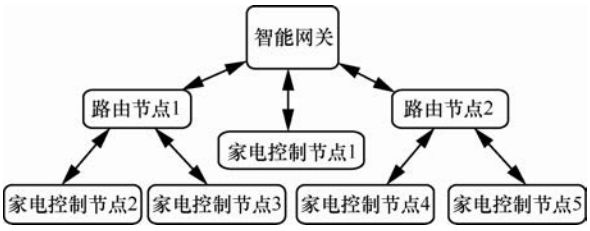

图 2　智能家居家庭内部无线网络拓扑结构

3　智能家居密钥管理机制

智能家居密钥管理机制由节点身份认证[6]，数据加密算法密钥的分布式产生与公钥发布、密钥安全存储、密钥更新，数字签名算法密钥的产生与分发、密钥安全存储等环节组成，即智能家居密钥管理机制包括数据加密算法的密钥管理机制和数字签名算法的密钥管理机制。

3.1　系统初始化

节点安装完成上电后，进行初始化，初始化包括各个节点参数的初始化以及硬件设置的

初始化，硬件的初始化是将片内闪存设置成读保护模式，对存储在其中的密钥进行硬件级别的安全保护。

3.1.1 设置 STM32 的片内闪存为读保护

使用系统启动程序 STM32 串口烧录程序将闪存设置为读保护，将寄存器的读保护选项字节设置为芯片保护（禁止调试和从 RAM 启动）。所有调试工具、内置 SRAM 或 FSMC 执行代码等方式对主存储器访问的操作将被禁止，只允许用户代码对主闪存的读操作和编程操作（除了闪存开始的 4 KB 区域不能编程）。

这样破解者将不能用调试工具、内置 SRAM 或者 FSMC 执行代码等方式读出闪存中的代码。破解者也不能使用系统启动程序读取代码，因为要解除读保护，将执行整个芯片的擦除操作。用户代码存储在 STM32 片内闪存中的数据在将得到硬件级别的保护。

3.1.2 读取 STM32 芯片的设备 ID

在主程序开始处中，加入对设备唯一 ID 的检测，只有读取出的 ID 与程序中存储的 ID 相同，才能继续执行主程序，否则，执行擦除操作。这样即使破解者复制出了芯片中的二进制码，也不能用这个二进制码去复制新的器件，从而伪造智能家居的节点，进入智能家居的无线网络中，从源头上制止了间谍节点的产生。具体实现方法如下。

- 在应用程序中定义一个（STM32 ID 为 96 位）const 变量，变量值全为 0xFF。每次启动程序时，检查 const 变量值，如果全为 0xFF，就读取器件的唯一 ID，通过闪存编程写入该 const 变量中（因为全是 0xFF，所以可以编程写入）。
- 在程序中多个地方检查 const 变量，如果变量值不为 0xFF 并且与设备 ID 不一致，就执行与功能无关代码（比如自擦除）。

这样，即使破解者读出了芯片中的二进制码，因为这个二进制码包含了设备唯一 ID，具有唯一性，所以不能复制到其他芯片中。

3.1.3 配置智能网关节点信息表

智能网关安装上电后，通过手机或者 PC 访问智能网关，将智能家居中的节点信息配置进智能网关的 STM32 的片内闪存（已进行读保护操作）中，智能家居节点信息见表 1。

表 1 智能家居节点信息

节点 STM32 ID 编号	节点功能编号	节点功能	数字签名随机数 r_i
96 bit 数据	GW	智能网关	r_1
96 bit 数据	R_1	路由节点 1	r_2
96 bit 数据	R_2	路由节点 2	r_3
96 bit 数据	HEA_1	家电控制节点 1	r_4
96 bit 数据	HEA_2	家电控制节点 2	r_5
96 bit 数据	HEA_3	家电控制节点 3	r_6
96 bit 数据	HEA_4	家电控制节点 4	r_7
96 bit 数据	HEA_5	家电控制节点 5	r_8

表 1 中的随机数 r_i 是由智能网关中的程序输入的，非人工输入，其他信息为人工输入，此表用于路由节点和家电控制节点与智能网关之间进行组网时的身份确认。

3.2 节点身份认证和组网

系统完成初始化后，路由节点和家电控制节点向外发送信息：AES（芯片 ID）||节点功能编号||消息的消息摘要（||表示将二进制数据连接起来），消息摘要是 AES（芯片 ID）||节点功能编号经过 SM3 散列函数运算后的输出值，可防止消息被篡改，节点功能编号是明码。此时的 AES 加密的密钥 K_A 是芯片 ID 经过 SM3 散列函数运算后的输出值的前 128 位（SM3 函数的输出值是 256 位）。

智能网关接收到其他节点发送的信息后，首先计算消息中相应部分的 SM3 散列值，并与接收的消息摘要进行对比，若相同，则说明消息没有被修改；接着提取信息中的节点功能编号（明码），在智能网关节点的 STM32F407 的片内闪存中查找节点功能编号对应的发送节点的芯片 ID，然后

将芯片 ID 经过 SM3 散列函数运算，提取 SM3 输出值的前 128 位作为 AED 加密的密钥 K_A，解密网关节点收到的对应的信息，获得发送节点的芯片 ID，将片内闪存查询到 ID 与解密获得的芯片 ID 对比，若相同，则网关确认拥有该芯片 ID 的节点合法，允许其接入网络，智能网关在完成所有节点的入网许可后，建立如图 2 所示拓扑结构的无线通信网络。节点身份认证的流程如图 3 所示。

3.3　数据加密算法的密钥管理机制

3.3.1　数据加密算法的密钥生成和分发

智能家居内部网络的拓扑结构形成后，每个节点知道其通信链路中相邻的节点是哪一个，每个节点产生自己的公钥私钥对，然后将公钥告知自己链路中相邻的节点，智能网关节点直接或者间接接收了所有路由和家电控制节点的公钥（即智能网关节点可以和所有节点进行保密通信），发送方节点利用接收方的公钥对信息进行加密，接收方节点收到信息后，利用自己的私钥对信息进行解密，获得信息内容。

密钥生成分为集中式密钥生成和分布式密钥生成两种模式，对于集中式，密钥由可信任的密钥管理中心生成；对于分布式，密钥由网络中的节点通过协商来完成[7]。本方案采用分布式密钥生成，具体的实施过程如下。

（1）在 FIPS.186-4（Federal Information Proc-

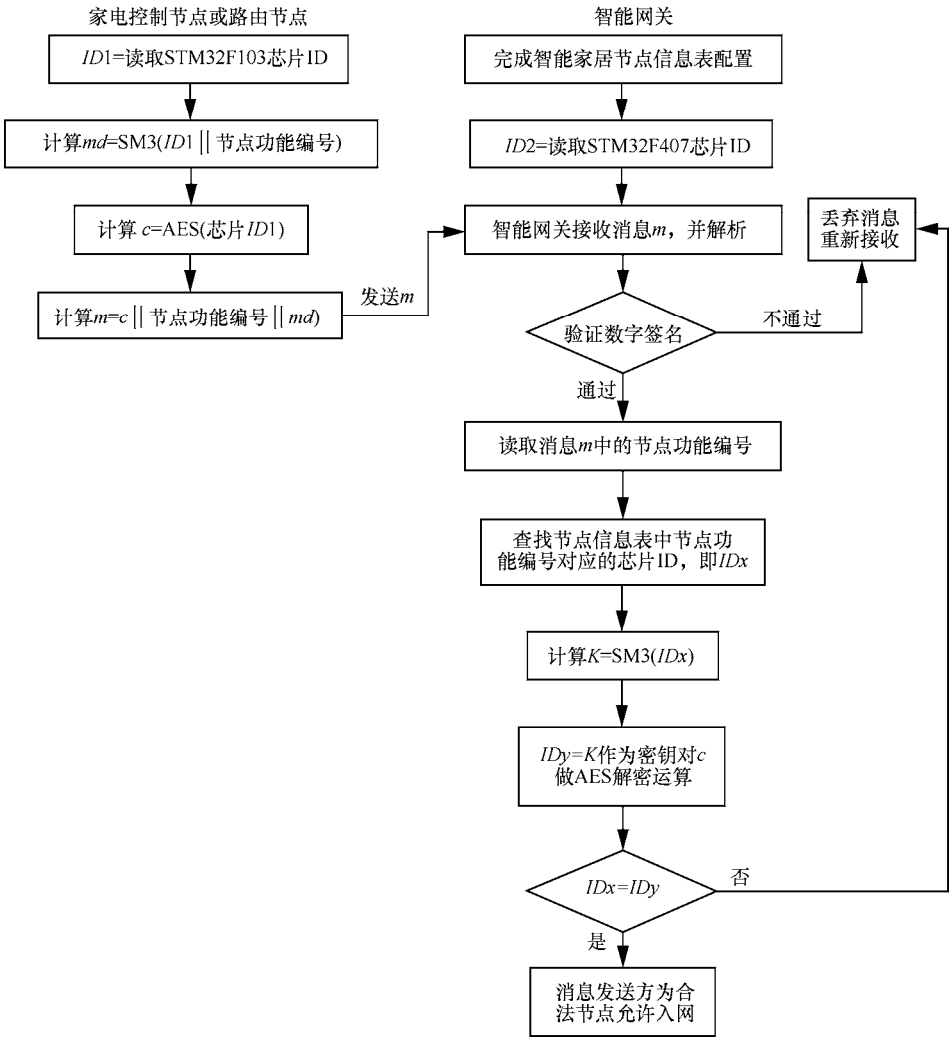

图 3　节点身份认证的流程

essing Standard，美国联邦信息处理标准）中，NIST（National Institute of Standard and Technology，美国国家标准与技术研究院）推荐了 15 个不同安全级别的椭圆曲线，本方案选择了素域 GF(q)上的椭圆曲线。

素域上的椭圆曲线表达式为：$y^2 \equiv x^3+ax+b \bmod q$，其中 q 为一个大素数，a、b、x、y 均在素域 GF(q)中，即从{0,1,⋯,q−1}上取值，且满足：$4a^2+27b^2 \neq 0 \bmod q$，$a$、$b$ 为椭圆曲线 $y^2 \equiv x^3+ax+b \bmod q$ 的系数，满足 $rb^2 \equiv a^3 \bmod q$，其中 $q=2^{194}-2^{64}-1$，$a=-3$，r=0x3099d2bb bfcb2538 542dcd5f b078b6ef 5f3d6fe2 c745de65。

基点 G 的阶 n=0xffffffff ffffffff ffffffff 99def836 146bc9b1 b4d22831。

基点 G 的坐标为：G_x=188da80e b03090f6 7cbf20eb 43a18800 f4ff0afd 82ff1012，G_y=07192b95 ffc8da78 631011ed 6b24cdd5 73f977a1 1e794811。

余因子 h=1（以上参数在 FIPS.186-4 中选择）。

（2）选择好椭圆曲线 E、基点 P 后，智能家居中每个节点随机产生一个安全私钥向量 $K^G=\{x_1,x_2,\cdots,x_h\}$，$x_j \in Z_q^*$（$h$ 为 SM3 散列函数输出结果的位数，Z_q^*为小于或等于 q 的正整数），公钥向量 $PK^G=\{x_1 \cdot P, x_2 \cdot P, \cdots, x_h \cdot P\}=\{P_1, P_2, \cdots, P_h\}$。

（3）每个节点设置一个初始的密钥发布时间 T_0（每个节点 T_0 可不同），节点的身份信息为 $ID=\{T_0 \| \text{STM32 ID}\}$，计算 h=SM3(ID)，h_l 表示 h 的第 l 位二进制，l=1,2,⋯,N；计算节点的公钥 $Y=\sum_{l=1}^{h} h_l P_l$，私钥为 $X=\sum_{l=1}^{h} h_l x_l$，可知 $Y=X \cdot P$。

（4）每个节点生成密钥后，计算 Y||SM3(Y)，向拓扑图中相邻的节点发送自己的公钥及公钥的消息摘要，路由节点收到公钥信息后会转发到智能网关，因此智能网关接收每个节点的公钥。节点收到公钥信息后，提取出节点公钥，将其存储在读保护设置的片内闪存中安全保存。

3.3.2 数据加密算法的密钥更新

智能家居家庭内部的无线网络组建后，数据加密算法的密钥使用频繁，为防止攻击者收集到足够的密文信息，破解数据加密密钥，因此，数据加密密钥需要定时更新，本方案在设计数据加密密钥时引入时间参数，将数据加密密钥设计成与时间相关的值，参照第 3.3.1 节中的步骤（3）可知，数据加密公钥和私钥都是与时间有关的值，同时数据加密公私密钥对是各个节点自己生成的，属于分布式密钥生成方式，只需要每个节点设置密钥更新周期，到达更新时间后，各个节点的密钥会自动更新，然后利用上文中的密钥分发技术分发公钥即可。

3.4 数字签名算法的密钥管理机制

数字签名算法利用节点的私钥进行签名，利用该节点的公钥进行验证。本文的数字签名的私钥由智能网关集中生成，再分发给各个节点，数字签名的公钥由节点利用私钥运算产生。

3.4.1 基于椭圆曲线的数字签名算法

本文的数字签名算法采用的是基于椭圆曲线的数字签名算法 ECDSA，其安全性已被 Brown 证明，具体的数字签名和验证签名过程如下。

（1）参数产生

需要发送信息的节点利用通信密钥的生成和分发中选择的椭圆曲线来产生需要的参数，需要发送信息的节点利用智能网关发送的随机数 r_i，计算 $Q=r_iG$，公钥为(n,Q)，私钥为 r_i。

（2）签名过程

①需要发送信息的节点利用 ANSI X9.17 标准化的伪随机数生成器产生一个随机数 k,$k \in [1,n-1]$，n 为选择的椭圆曲线基点 G 的阶，计算 $kG=(x,y)$，$t=x \bmod n$。

②计算 $e=h(m)$，h 为 SM3 散列函数。

③计算 $s=(e+td)\,k-1 \bmod n$。若 t=0 或 s=0，则转回①，消息 m 的签名为(r,t)。

（3）数字签名验证过程

①计算 e=SM3(m)。

②计算

$$u=s^{-1}e \bmod n \quad (1)$$

$$v=s^{-1}e \bmod n \quad (2)$$

$$(x-1,y-1)=uG+vQ \quad (3)$$

$$t'=x' \bmod n \quad (4)$$

③若 $t=t'$，则签名有效，否则无效。

3.4.2　数字签名算法的密钥生成与分发

节点经过身份验证后，组成以智能网关为根节点的无线网络，拓扑结构已经形成，每个节点生成自己的数据加密算法的公私密钥对，且告知了拓扑相邻节点自己的公钥，智能网关保存了所有节点的公钥。智能网关利用 ANSI X9.17 标准化的伪随机数生成器生成每个节点所需的数字签名随机数 $r_i(i=1,2,\cdots,8)$，$r_i \in [1,n-1]$，n 为选择的椭圆曲线基点 G 的阶，智能网关将每个节点的随机数存入智能家居节点信息表中，即表 1。数字签名算法的私钥由智能网关集中生成，数字签名算法的公钥则由节点利用随机数 r_i 运算产生。智能网关用节点的数据加密公钥 Y_i 加密对应节点的随机数 r_i，并发送给对应节点，节点收到信息后，利用私钥解密，获取自己的数字签名随机数 r_i。完成以上步骤后，各个节点获得数据加密算法的公私密钥对和数字签名算法所需的随机数 r_i，各个节点之间通信的信息利用椭圆曲线加密算法加密，保证信息的保密性，利用 ECDSA 数字签名算法签名和验证，保证信息的不可抵赖性和不可伪造性。

3.4.3　数字签名算法的密钥更新

数字签名算法的私钥为智能网关生成的随机数 r_i，为集中式生成方式，数字签名算法的公钥为节点收到本节点的随机数 r_i 后，通过运算生成，因此数字签名算法的密钥更新由智能家居重新生成随机数，再分发给各个节点，节点获得本节点的私钥，利用私钥即可运算出本节点的公钥。

3.5　新节点加入机制

在新节点加入之前，需要在智能网关中人工配置节点信息，即表 1 中所示节点信息，同样，接着新加入节点执行第 3.1~3.4 节中的步骤，从节点初始化、身份认证到数字签名，完成这些步骤后，新加入节点即可在无线网络中实现安全通信，同时，新加入节点也设置了密钥定期更新，防止攻击者收集足够的密文，破解密钥。本方案为新节点的加入提供了便利，实现本方案的可扩展性。

4　密钥管理机制性能分析

4.1　安全性

本方案采用了基于椭圆曲线的数据加密和数字签名方案，基于椭圆曲线的密码方案具有密钥短、存储空间小、计算速度快、软硬件实现节省资源的优势，适合在计算能力和存储空间有限，带宽受限的场景中应用。本方案选取的椭圆曲线是 NIST 的 FIPS.186-4 中推荐的椭圆曲线，密钥的位数为 192 位，密钥长度安全性得到了 NIST 的测试，安全性足够。在存储数据时将机密数据（如密钥等）加密后存储在设置为读保护的片内闪存中，实现了硬件级别的保护，同时将芯片 ID 设置为节点程序运行时的检查参数，读取的芯片 ID 与程序中已有的 ID 值不同时，程序将执行擦除操作，将程序从芯片中擦除，保证了攻击者不能将节点复制，即智能家居中的每个节点都是独一无二的，智能家居的所有节点都在家庭内部，攻击者获得智能家居节点的难度大，保证了节点的难获取性。

数据加密的密钥采用分布式产生的方式，节点自己生成自己的公钥私钥对，防止了集中式生成密钥方式的单点失效；数字签名的密钥采用集中式和分布式结合的方式产生，私钥集中由智能网关产生，公钥由各个节点自己产生。密钥存储在读保护的闪存中，保证了密钥的安全存储。

数据加密和数字签名的密钥均为定时更新，保证了攻击者不能收集足够的密文信息对密钥进行破解。

4.2　耗时分析

无线网络密钥管理方案中的经典方案是 Eschenauer 和 Gligor 提出的一种基于随机概率的

无线网络密钥管理方案，即 E-G 密钥管理方案。该方案的密钥分配由 3 个阶段组成，分别是密钥的预分发阶段、直接密钥协商阶段（间接密钥协商阶段）、路径密钥的建立阶段。该方案的基本思路是：基站预先生成一个大的密钥池，保存整个网络中所需的原始密钥，然后为每个节点随机分配一定数量的密钥，只要任意两个节点有一对相同的密钥，这两个节点之间就可以建立起安全的通信链路。该方案采用密钥集中生成的方式，而本文的加密密钥是分布式生成的，即节点自己产生自己的密钥，密钥无需分发。该方案的密钥数量也较大，本文的密钥数量相对少很多。E-G 方案在密钥协商阶段耗时长，而本文的密钥管理方案没有密钥协商环节，因此耗时短。本文的密钥管理方案和 E-G 密钥管理方案的耗时对比如图 4 所示。因此本文的密钥管理机制相对于 E-G 方案具有密钥无需分发、密钥数量少、耗时短的优点。

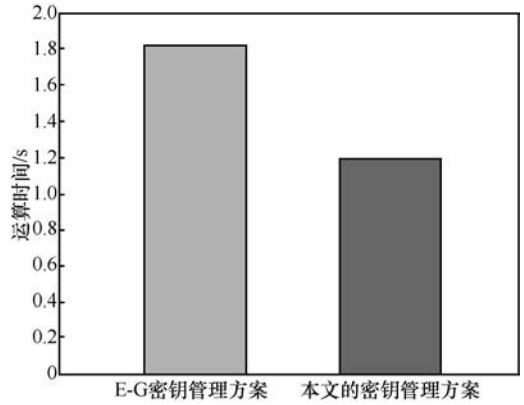

图 4　本文的密钥管理方案和 E-G 密钥管理方案的耗时对比

4.3　可扩展性

智能家居内部无线网络在组建完成后，如果有新的节点加入，则新加入节点执行第 3.1~3.4 节中的步骤，这些步骤都经过安全设计，保证了合法节点才能加入网络，同时合法节点加入网络也很便捷，保证了这个方案良好的可扩展性。

5　结束语

本文设计了一种适合智能家居内部网络使用的基于椭圆曲线密码体制的密钥管理机制，并详细讨论了机制的工作原理，分析了密钥管理机制的安全性和可扩展性。在下一步的工作中，会进一步完善密钥管理机制，提高安全性，同时，降低方案的复杂程度。

参考文献：

[1] PIRBHULAL S, ZHANG H, ALAHI M E, et al. A novel secure IoT-based smart home automation system using a wireless sensor network[J]. Sensors, 2016, 17(1): 69.

[2] LU Y R, LI L X, PENG H P, et al. An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography[J]. Multimedia Tools & Applications, 2017, 76(2): 1801-1815.

[3] ALTOP D K, BINGÖL M A, LEVI A, et al. DKEM: secure and efficient distributed key establishment protocol for wireless mesh networks[J]. Ad Hoc Networks, 2016(54): 53-68.

[4] ABDALLA M, BENHAMOUDA F, POINTCHEVAL D. Public-key encryption indistinguishable under plaintext-checkable attacks[J]. Iet Information Security, 2016, 10(6): 288-303.

[5] 金宁, 张道远, 高建桥, 等. 对称密码和非对称密码算法在无线传感器网络中应用研究[J]. 传感技术学报, 2011, 24(6): 874-878.
JIN N, ZHANG D Y, GAO J Q, et al. A study on the application of symmetric ciphers and asymmetric ciphers in wireless networks[J]. Chinese Journal of Sensors and Actuators, 2011, 24(6): 874-878.

[6] 王崇霞, 高美真, 刘倩, 等. 混合云联合身份认证与密钥协商协议设计[J]. 电信科学, 2014, 30(4): 95-99, 108.
WANG C X, GAO M Z, LIU Q, et al. Design of united identity authentication and key agreement protocol for hybrid cloud[J]. Telecommunications Science, 2014, 30(4): 95-99, 108.

[7] 任伟. 现代密码学[M]. 北京: 北京邮电大学出版社, 2011.
REN W. Modern cryptography[M]. Beijing: Beijing University of Posts and Telecommunications Press, 2011.

[作者简介]

程文彬（1965−），男，电子科技大学中山学院副教授，主要研究方向为物联网、智能家居、无线传感器及其网络等。

刘佳（1989−），男，电子科技大学机械电子工程学院硕士生，主要研究方向为物联网、智能家居。