(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109756877 A
(43)申请公布日 2019.05.14

(21)申请号 201811482918.9

(22)申请日 2018.12.05

(71)申请人 西安电子科技大学
地址 710071 陕西省西安市太白南路2号西安电子科技大学

(72)发明人 曹进 于璞 李晖 赵兴文

(74)专利代理机构 西安长和专利代理有限公司 61227
代理人 黄伟洪

(51)Int.Cl.
H04W 4/80(2018.01)
H04W 12/02(2009.01)
H04W 12/06(2009.01)
H04W 28/10(2009.01)

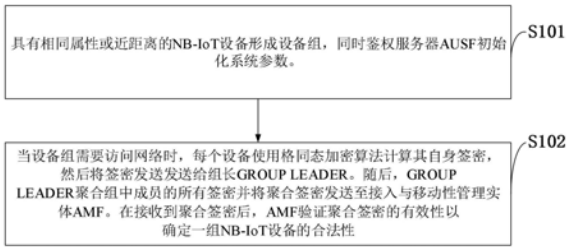
权利要求书3页 说明书9页 附图1页

(54)发明名称

一种海量NB-IoT设备的抗量子快速认证与数据传输方法

(57)摘要

本发明属于通信网络安全技术领域，公开了一种海量NB-IoT设备的抗量子快速认证与数据传输方法；具有相同属性或近距离的NB-IoT设备形成设备组，当设备组需要访问网络时，每个设备使用格同态加密算法计算其自身签密；将签密发送发送给组长GROUP LEADER。随后，GROUP LEADER聚合组中成员的所有签密并将聚合签密发送至接入与移动性管理实体AMF；在接收到聚合签密后，AMF验证聚合签密的有效性以确定一组NB-IoT设备的合法性。本发明可以基于格的同态加密技术同时实现一组NB-IoT设备的接入认证与数据传输而无需建立数据承载，简化信令流；与现有技术相比，认证与数据传输成本较低。



CN 109756877 A

1.一种海量NB-IoT设备的抗量子快速认证与数据传输方法,其特征在于,所述海量NB-IoT设备的抗量子快速认证与数据传输方法具有相同属性或近距离的NB-IoT设备形成设备组,当设备组需要访问网络时,每个设备使用格同态加密算法计算其自身签密;然后将签密发送发送给组长GROUP LEADER;GROUP LEADER聚合组中成员的所有签密并将聚合签密发送至接入与移动性管理实体AMF;在接收到聚合签密后,AMF验证聚合签密的有效性以确定一组NB-IoT设备的合法性。

2.如权利要求1所述的海量NB-IoT设备的抗量子快速认证与数据传输方法,其特征在于,所述海量NB-IoT设备的抗量子快速认证与数据传输方法包括以下步骤:

步骤一,系统初始化阶段;

步骤二,基于群组的快速认证与数据传输阶段。

3.如权利要求2所述的海量NB-IoT设备的抗量子快速认证与数据传输方法,其特征在于,所述步骤一具体包括:

(1)鉴权服务器AUSF计算系统参数$m=\lceil 6nlogq\rceil$与$l=O(\sqrt{nlogq})$,其中n为系统安全参数,q为系统安全参数n的多项式,符号$\lceil x\rceil$表示不大于x的整数,符号O(f(n))为关于系统安全参数n函数的复杂度;

(2)鉴权服务器AUSF设置聚合高斯参数$s_a \geq l\cdot\omega(\sqrt{logm})$,接入与移动性管理实体AMF高斯参数$s_{AMF}\geq l\cdot\omega(\sqrt{logm})$与窄带物联网NB-IoT设备高斯参数$s_i\geq l\cdot\omega(\sqrt{logm})$,i=1,2...t,其中t为NB-IoT设备数量,符号ω(f(m))为关于系统参数m函数的复杂度;同时鉴权服务器AUSF利用算法TrapGen(n,q,m)获得均匀随机矩阵A_a与基于矩阵A_a生成的格$\Lambda_q^{\perp}(A_a)$中的短基T_a,其中算法TrapGen(n,q,m)为多项式时间陷门生成算法;输入参数为系统安全参数n,系统安全参数n的多项式q与系统参数m,输出参数为均匀随机矩阵A_a与短基T_a;

(3)鉴权服务器AUSF设置t个格Λ_i以满足等式$\Lambda_1+\Lambda_2+...+\Lambda_t=Z^m$和等式$\Lambda_1\cap\Lambda_2\cap...\cap\Lambda_t=\Lambda_q^{\perp}(A_a)$,其中$Z^m$为整数集上的n阶向量,符号∩为交集,$\Lambda_q^{\perp}(A_a)$为基于矩阵$A_a$生成的格;

(4)当NB-IoT设备$IOTD_i$接入5G网络时,5G接入与移动性管理实体AMF对每个设备$IOTD_i$通过执行认证与密钥协商协议5G AKA或EAP AKA'以完成初始认证;

(5)在成功完成初始认证后,鉴权服务器AUSF利用算法TrapGen(n,q,m)为每个NB-IoT设备$IOTD_i$生成一个公钥/私钥对(A_i,T_i)并安全地分配给每个NB-IoT设备$IOTD_i$,其中算法TrapGen(n,q,m)为多项式时间算法,公钥A_i为均匀随机矩阵,私钥T_i为基于矩阵A_i生成的格$\Lambda_q^{\perp}(A_i)$中的短基T_i;

(6)在成功完成初始认证后,鉴权服务器AUSF利用算法TrapGen(n,q,m)为每个接入与移动性管理实体AMF生成一个公钥/私钥对(A_{AMF},T_{AMF})并安全地分配给每个接入与移动性管理实体AMF,其中算法TrapGen(n,q,m)为多项式时间算法,公钥A_{AMF}为均匀随机矩阵,私钥T_{AMF}为基于矩阵A_{AMF}生成的格$\Lambda_q^{\perp}(A_{AMF})$中的短基$T_{AMF}$。

4.如权利要求2所述的海量NB-IoT设备的抗量子快速认证与数据传输方法,其特征在

于,所述步骤二具体包括:

(1)每个NB-IoT设备$IOTD_i$准备其将要发送的明文数据向量$U_i = PDU_i \parallel ID_{IOTD_i} \parallel GID = (U_1, ..., U_m)^T$,其中$PDU_i$为协议数据单元,$ID_{IOTD_i}$为NB-IoT设备的身份,GID为NB-IoT设备群组的身份;然后每个NB-IoT设备$IOTD_i$利用目标接入与移动性管理实体AMF的公钥A_{AMF}计算密文$C_i = A_{AMF} * U_i$;同时每个NB-IoT设备$IOTD_i$利用多项式时间算法SamplePre与自身私钥T_i生成签名$Y_i = (e_i, x_i)$,其中$e_i = SamplePre(A_i, T_i, H_1(x_i), s_i)$为算法SamplePre输出结果,$x_i$为随机数,$H_1$为哈希函数,$s_i$为高斯参数;每个NB-IoT设备$ID_{IOTDi}$构造一个接入请求信息将$(C_i, Y_i)$发送给设备组组长GROUP LEADER;

(2)设备组组长GROUP LEADER在成功接收到组内所有NB-IoT设备的接入请求后执行以下步骤:

1)利用每个NB-IoT设备的部分签名e_i与t个格Λ_i计算部分聚合签名$e = e_1 \bmod \Lambda_1$,$e = e_2 \bmod \Lambda_2$,...,$e = e_t \bmod \Lambda_t$;

2)利用多项式时间算法SampleGaussian计算部分聚合签名$e_0 = SampleGaussian(T_a, s_a, --e)$,其中$T_a$为基于矩阵Aa生成的格$\Lambda_q^{\perp}(A_a)$中的短基,$s_a$为高斯参数,e为部分聚合签名;

3)利用计算出的部分聚合签名e,e_0计算聚合签名$e_a = e_0 + e$;

4)构造一个聚合接入请求信息将$(e_a, \{C_i, x_i\}_{i=1}^t)$发送给5G网络中的目标接入与移动性管理实体AMF,其中e_a为聚合签名,C_i为每个NB-IoT设备生成的密文,x_i为每个NB-IoT设备生成的随机数;

(3)接入与移动性管理实体AMF在成功接收到设备组组长发送的聚合接入请求后执行以下步骤:

1)验证聚合签名e_a是否合法,验证公式为下述公式(A)与公式(B):

$$\| e_a \| \leq s_a \sqrt{m} \qquad (A)$$

$$H_2(H_1(x_1), H_1(x_2) ... H_1(x_t)) = H_2(A_1(e_a \bmod \Lambda_1) \bmod q, ..., A_t(e_a \bmod \Lambda_t) \bmod q) \qquad (B)$$

其中e_a为聚合签名,s_a为高斯参数,m,q为系统参数,H_1,H_2为哈希函数,x_i为NB-IoT设备生成的随机数,A_i为均匀随机矩阵,Λ_i为格;

2)若上述聚合签名是合法的,接入与移动性管理实体AMF利用多项式时间算法SamplePre与自身私钥T_{AMF}解密出每个NB-IoT发送的明文数据$U_i = SamplePre(A_{AMF}, T_{AMF}, C_i, s_{AMF})$,其中$A_{AMF}$为接入与移动性管理实体AMF的公钥,$C_i$为密文,$s_{AMF}$为高斯参数;同时生成一个随机的认证成功标识符Succ;

3)利用多项式时间算法SamplePre与自身私钥T_{AMF}生成签名$Y_{AMF} = SamplePre(A_{AMF}, T_{AMF}, H_1(Succ), s_{AMF})$,其中$A_{AMF}$为AMF的公钥,$H_1$为哈希函数,$s_{AMF}$为高斯参数;

4)若此时AMF有需要发送的下行数据,则利用每个NB-IoT设备的公钥A_i加密下行数据密文$C_{AMF} = A_i * PDU_{AMF}$,其中$PDU_{AMF}$为协议数据单元;

5)构造一个聚合接入响应信息将$(ID_{AMF}, Y_{AMF}, C_{AMF}, Succ)$发送给目标设备组组长GROUP LEADER,其中ID_{AMF}为AMF的身份,Y_{AMF}为AMF生成的签名,C_{AMF}为下行数据密文,Succ为认证成功标识符;

(4)目标设备组组长GROUP LEADER在成功接收到聚合接入响应信息后将接入响应信息发分发到小组内每个目标NB-IoT设备；

(5)小组内每个目标NB-IoT设备在成功接收到接入认证响应信息后执行以下步骤：

1)验证AMF生成的签名Y_{AMF}是否合法，验证公式为下述公式(C)与公式(D)：

$A_{AMF}Y_{AMF}=H_1(Suce)$ (C)

$$\| Y_{AMF} \| \leq s_{AMF}\sqrt{m} \qquad (D)$$

其中A_{AMF}为AMF的公钥，$H_1(Succ)$为经过哈希函数H_1计算的成功标识符，s_{AMF}为高斯参数，m为系统参数；

2)若上述AMF的签名Y_{AMF}是合法的，则利用多项式时间算法SamplePre与自身私钥T_i解密下行数据密文C_{AMF}从而获得下行数据明文$PDU_{AMF}=SamplePre(A_i,T_i,C_{AMF},s_i)$，其中$A_i$为每个NB-IoT设备的公钥，$s_i$为高斯参数。

5.一种应用权利要求1～4任意一项所述海量NB-IoT设备的抗量子快速认证与数据传输方法的移动通信控制系统。

6.一种应用权利要求1～4任意一项所述海量NB-IoT设备的抗量子快速认证与数据传输方法的5G通信平台。

一种海量NB-IoT设备的抗量子快速认证与数据传输方法

技术领域

[0001] 本发明属于通信网络安全技术领域，尤其涉及一种海量NB-IoT设备的抗量子快速认证与数据传输方法。

背景技术

[0002] 目前，业内常用的现有技术是这样的：随着移动通信技术的不断发展，第三代合作伙伴计划(3GPP)已经提出了与第五代移动通信技术(5G)相关的标准，这标志着当前长期演进系统(LTE-A)到下一代移动通信网络5G系统演进的正式开始。在未来的5G网络中，窄带物联网(NB-IoT)系统已成为万物互联的重要分支。3GPP委员会提出了NB-IoT系统的核心标准。这些核心标准的出现使每个符合条件的物联网终端能够通过3GPP接入网络安全地接入5G核心网络。由于未来5G网络中的更高容量和更低传输延迟等性能特性，这将成为NB-IoT系统的重要机会。NB-IoT功耗低，覆盖范围广，成本低，容量大，可广泛应用于各种垂直行业，如远程抄表，资产跟踪，智能停车，智能农业等。目前，全球移动运营商和制造公司正在积极开展NB-IoT系统的研发和推广。如今，部署在LTE-A网络上的NB-IoT系统已经完善。然而，部署在5G网络中的NB-IoT系统仍处于初期和研究阶段。由于NB-IoT设备的海洋具有资源有限，动态拓扑变化，复杂网络环境，以数据为中心和密切相关的应用的特点，因此需要有效的接入认证和数据分配方案来确保NB-IoT系统的安全性。3GPP委员会指出，现有的协议中每个NB-IoT设备需要执行基本的认证与密钥协商(5G-AKA)或(EAP-AKA')过程，以实现与3GPP核心网络的相互认证。在与3GPP核心网络建立安全连接之后秘密地执行数据传输。该过程需要多轮信令交换，并且导致大量的信令开销和通信开销。特别是，大规模的NB-IoT设备同时连接到5G核心网络，这将导致网络节点严重的网络拥塞，严重影响NB-IoT系统的服务质量(QoS)。当前于传统的LTE系统中已经给出了多种基于群组的接入聚合认证协议，但是这些协议还存在很多漏洞。首先，这些认证协议都不能抵抗量子攻击；其次，由于密码方案的安全性，如众所周知的RSA公钥加密系统，Diffie-Hellman密钥交换和椭圆曲线加密(ECC)系统大多基于离散对数问题或大整数分解问题，量子计算机可以有效地处理这些问题。因此，如何实现5G网络中海量NB-IoT设备的快速认证与数据传输是当前面临的一个关键问题。将基于格的同态加密技术引入5G网络中的NB-IoT系统将大大简化信令流并提供强大的安全属性。通过这种方法，5G网络中可以同时实现一组NB-IoT设备的接入认证与数据传输而无需建立数据承载。但是由于此研究还处于初级阶段，目前还没有5G网络中针对海量NB-IoT设备的快速认证与数据传输的相关研究。

[0003] 综上所述，目前没有5G网络中针对海量NB-IoT设备的快速认证与数据传输的有效机制。原因有以下几点：第一，目前对5G网络中NB-IoT系统的接入认证与数据传输研究仍处于初级阶段；第二，现有技术存在问题需要解决，一方面，NB-IoT设备需要从空闲状态进入连接状态以发送或接收几个字节的数据，其中消耗的网络信令开销可能远大于接收/发送数据本身的大小；另一方面，完整的基本认证与密钥协商协议(EAP-AKA')或(5G-AKA)过程以及IP或非IP数据传输过程由每个活动的NB-IoT设备实现。上述两个过程的执行可能在资

源受限的NB-IoT设备上引起大量的信令和通信开销。此外，业内常用的现有技术主要依赖于诸如椭圆曲线密码系统(ECC)等加密算法作为基础来保证NB-IoT系统的安全。然而，像ECC、RSA以及DH密钥交换协议这样的公钥方案很容易被即将推出的量子计算机打破。解决这一系列问题的难度主要在于NB-IoT系统具有资源有限，动态拓扑变化，复杂网络环境，以数据为中心和密切相关的应用的特点以及如何将抗量子加密算法应用到未来5G网络中的NB-IoT系统当中。本发明的方法主要有以下意义：

[0004] 1)本发明中的方法为大规模NB-IoT设备提出快速访问认证和数据分发方案。该方案可以同时实现一组NB-IoT设备与5G核心网之间的相互认证和数据传输过程。

[0005] 2)本发明中的方法可以实现强大的安全保护，包括抵抗量子攻击，保护了用户身份的隐私性，数据的机密性与完整性，数据的不可伪造性与抵抗重放攻击。

[0006] 3)与其他现有传统的认证协议相比，本发明中的方法大大减少了信令开销和通信开销。

发明内容

[0007] 针对现有技术存在的问题，本发明提供了一种海量NB-IoT设备的抗量子快速认证与数据传输方法。

[0008] 本发明是这样实现的，一种海量NB-IoT设备的抗量子快速认证与数据传输方法，所述海量NB-IoT设备的抗量子快速认证与数据传输方法具有相同属性或近距离的NB-IoT设备形成设备组，当设备组需要访问网络时，每个设备使用格同态加密算法计算其自身签密；然后将签密发送发送给组长GROUP LEADER；GROUP LEADER聚合组中成员的所有签密并将聚合签密发送至接入与移动性管理实体AMF；在接收到聚合签密后，AMF验证聚合签密的有效性以确定一组NB-IoT设备的合法性。

[0009] 进一步，所述海量NB-IoT设备的抗量子快速认证与数据传输方法包括以下步骤：

[0010] 步骤一，系统初始化阶段；

[0011] 步骤二，基于群组的快速认证与数据传输阶段。

[0012] 进一步，所述步骤一具体包括：

[0013] (1)鉴权服务器AUSF计算系统参数$m=\lceil 6nlogq\rceil$与$l=O(\sqrt{nlogq})$，其中n为系统安全参数，q为系统安全参数n的多项式，符号$\lceil x\rceil$表示不大于x的整数，符号O(f(n))为关于系统安全参数n函数的复杂度；

[0014] (2)鉴权服务器AUSF设置聚合高斯参数$s_a \geq l\cdot\omega(\sqrt{logm})$，接入与移动性管理实体AMF高斯参数$s_{AMF} \geq l\cdot\omega(\sqrt{logm})$与窄带物联网NB-IoT设备高斯参数$s_i \geq l\cdot\omega(\sqrt{logm}), i=1,2...t$，其中t为NB-IoT设备数量，符号ω(f(m))为关于系统参数m函数的复杂度；同时鉴权服务器AUSF利用算法TrapGen(n,q,m)获得均匀随机矩阵A_a与基于矩阵A_a生成的格$\Lambda_q^{\perp}(A_a)$中的短基T_a，其中算法TrapGen(n,q,m)为多项式时间陷门生成算法；输入参数为系统安全参数n，系统安全参数n的多项式q与系统参数m，输出参数为均匀随机矩阵A_a与短基T_a；

[0015] (3)鉴权服务器AUSF设置t个格Λ_i以满足等式$\Lambda_1+\Lambda_2+...+\Lambda_t=Z^m$和等式

$\Lambda_1 \cap \Lambda_2 \cap ... \cap \Lambda_t = \Lambda_q^{\perp}(A_a)$，其中$Z^m$为整数集上的n阶向量，符号∩为交集，$\Lambda_q^{\perp}(A_a)$为基于矩阵$A_a$生成的格；

[0016] (4)当NB-IoT设备$IOTD_i$接入5G网络时，5G接入与移动性管理实体AMF对每个设备$IOTD_i$通过执行认证与密钥协商协议5GAKA或EAPAKA'以完成初始认证；

[0017] (5)在成功完成初始认证后，鉴权服务器AUSF利用算法TrapGen(n,q,m)为每个NB-IoT设备$IOTD_i$生成一个公钥/私钥对(A_i,T_i)并安全地分配给每个NB-IoT设备$IOTD_i$，其中算法TrapGen(n,q,m)为多项式时间算法，公钥A_i为均匀随机矩阵，私钥T_i为基于矩阵A_i生成的格$\Lambda_q^{\perp}(A_i)$中的短基T_i；

[0018] (6)在成功完成初始认证后，鉴权服务器AUSF利用算法TrapGen(n,q,m)为每个接入与移动性管理实体AMF生成一个公钥/私钥对(A_{AMF},T_{AMF})并安全地分配给每个接入与移动性管理实体AMF，其中算法TrapGen(n,q,m)为多项式时间算法，公钥A_{AMF}为均匀随机矩阵，私钥T_{AMF}为基于矩阵A_{AMF}生成的格$\Lambda_q^{\perp}(A_{AMF})$中的短基$T_{AMF}$。

[0019] 进一步，所述步骤二具体包括：

[0020] (1)每个NB-IoT设备$IOTD_i$准备其将要发送的明文数据向量$U_i = PDU_i \parallel ID_{IOTD_i} \parallel GID = (U_1,...,U_m)^T$，其中$PDU_i$为协议数据单元，$ID_{IOTD_i}$为NB-IoT设备的身份，GID为NB-IoT设备群组的身份；然后每个NB-IoT设备$IOTD_i$利用目标接入与移动性管理实体AMF的公钥A_{AMF}计算密文$C_i = A_{AMF} * U_i$；同时每个NB-IoT设备$IOTD_i$利用多项式时间算法SamplePre与自身私钥T_i生成签名$Y_i = (e_i, x_i)$，其中e_i = SamplePre$(A_i, T_i, H_1(x_i), s_i)$为算法SamplePre输出结果，$x_i$为随机数，$H_1$为哈希函数，$s_i$为高斯参数；每个NB-IoT设备$ID_{IOTD_i}$构造一个接入请求信息将$(C_i,Y_i)$发送给设备组组长GROUP LEADER；

[0021] (2)设备组组长GROUP LEADER在成功接收到组内所有NB-IoT设备的接入请求后执行以下步骤：

[0022] 1)利用每个NB-IoT设备的部分签名e_i与t个格Λ_i计算部分聚合签名$e = e_1 \bmod \Lambda_1$，$e = e_2 \bmod \Lambda_2, \cdots, e = e_t \bmod \Lambda_t$；

[0023] 2)利用多项式时间算法SampleGaussian计算部分聚合签名e_0 = SampleGaussian$(T_a, s_a, -e)$，其中T_a为基于矩阵A_a生成的格$\Lambda_q^{\perp}(A_a)$中的短基，s_a为高斯参数，e为部分聚合签名；

[0024] 3)利用计算出的部分聚合签名e，e_0计算聚合签名$e_a = e_0 + e$；

[0025] 4)构造一个聚合接入请求信息将$(e_a, \{C_i, x_i\}_{i=1}^t)$发送给5G网络中的目标接入与移动性管理实体AMF，其中e_a为聚合签名，C_i为每个NB-IoT设备生成的密文，x_i为每个NB-IoT设备生成的随机数；

[0026] (3)接入与移动性管理实体AMF在成功接收到设备组组长发送的聚合接入请求后执行以下步骤：

[0027] 1)验证聚合签名e_a是否合法，验证公式为下述公式(A)与公式(B)：

[0028] $$\parallel e_a \parallel \leq s_a\sqrt{m} \qquad (A)$$

[0029] $H_2(H_1(x_1); H_1(x_2) \ldots H_1(x_t))$

[0030] $=H_2(A_1(e_a \bmod \Lambda_1) \bmod q, \ldots, A_t(e_a \bmod \Lambda_t) \bmod q)$ (B)

[0031] 其中e_a为聚合签名，s_a为高斯参数，m，q为系统参数，H_1，H_2为哈希函数，x_i为NB-IoT设备生成的随机数，A_i为均匀随机矩阵，Λ_i为格；

[0032] 2)若上述聚合签名是合法的，接入与移动性管理实体AMF利用多项式时间算法SamplePre与自身私钥T_{AMF}解密出每个NB-IoT发送的明文数据U_i＝SamplePre(A_{AMF}，T_{AMF}，C_i，s_{AMF})，其中A_{AMF}为接入与移动性管理实体AMF的公钥，C_i为密文，s_{AMF}为高斯参数；同时生成一个随机的认证成功标识符Succ；

[0033] 3)利用多项式时间算法SamplePre与自身私钥T_{AMF}生成签名Y_{AMF}＝SamplePre(A_{AMF}，T_{AMF}，H_1(Succ)，s_{AMF})，其中A_{AMF}为AMF的公钥，H_1为哈希函数，s_{AMF}为高斯参数；

[0034] 4)若此时AMF有需要发送的下行数据，则利用每个NB-IoT设备的公钥A_i加密下行数据密文C_{AMF}＝A_i*PDU_{AMF}，其中PDU_{AMF}为协议数据单元；

[0035] 5)构造一个聚合接入响应信息将(ID_{AMF}，Y_{AMF}，C_{AMF}，Succ)发送给目标设备组组长GROUP LEADER，其中ID_{AMF}为AMF的身份，Y_{AMF}为AMF生成的签名，C_{AMF}为下行数据密文，Succ为认证成功标识符；

[0036] (4)目标设备组组长GROUP LEADER在成功接收到聚合接入响应信息后将接入响应信息发分发到小组内每个目标NB-IoT设备；

[0037] (5)小组内每个目标NB-IoT设备在成功接收到接入认证响应信息后执行以下步骤：

[0038] 1)验证AMF生成的签名Y_{AMF}是否合法，验证公式为下述公式(C)与公式(D)：

[0039] $A_{AMF}Y_{AMF}=H_1(\text{Succ})$ (C)

[0040] $$\| Y_{AMF} \| \leq s_{AMF}\sqrt{m} \qquad (D)$$

[0041] 其中A_{AMF}为AMF的公钥，H_1(Succ)为经过哈希函数H_1计算的成功标识符，s_{AMF}为高斯参数，m为系统参数；

[0042] 2)若上述AMF的签名Y_{AMF}是合法的，则利用多项式时间算法SamplePre与自身私钥T_i解密下行数据密文C_{AMF}从而获得下行数据明文PDU_{AMF}＝SamplePre(A_i，T_i，C_{AMF}，s_i)，其中A_i为每个NB-IoT设备的公钥，s_i为高斯参数。

[0043] 本发明的另一目的在于提供一种应用所述海量NB-IoT设备的抗量子快速认证与数据传输方法的移动通信控制系统。

[0044] 本发明的另一目的在于提供一种应用所述海量NB-IoT设备的抗量子快速认证与数据传输方法的5G通信平台。

[0045] 综上所述，本发明的优点及积极效果为：相互认证：在本发明的方法中，实现了NB-IoT设备组和接入与移动性管理实体AMF之间的相互认证；一方面，只有合法的NB-IoT设备$IOTD_i$可以导出合法签密，由设备组组长GROUP LEADER生成正确的聚合签密。如果没有私钥T_i，T_{AMF}，攻击者就无法获得有效的签密和聚合签密。另一方面，NB-IoT设备可以通过验证AMF生成的签密Y_{AMF}来检查AMF是否合法。.

[0046] 抵抗协议攻击：在本发明提出的方法中，由于格同态加密，本发明提出的方法可以抵抗量子攻击。此外，任何攻击者都无法在不获取私钥T_i，T_{AMF}的情况下伪造合法签密和合法聚合签密，因此本发明提出的方法具有不可伪造性。此外，在本发明提出的方法中，将随机数x添加到签密的生成中，因此本发明提出的方法可以抵抗重放攻击。

[0047] 用户身份信息保护:在本发明的方法中,每个NB-IoT设备的身份ID_{IOTD_i}都是使用接入与移动性管理实体AMF的公钥A_{AMF}加密和传输的。如果攻击者没有获得AMF的秘密私钥T_{AMF},则该消息无法解密,因此无法获取。

[0048] 数据保密性与完整性:在本发明的方法中,通过使用格同态加密技术来确保数据传输过程的安全性。如果没有接入与移动性管理实体AMF的私钥T_{AMF},任何攻击者都无法解密数据。同时,本发明的方法中通过使用数字签名技术来确保数据传输过程中传输数据的完整性。只有合法的NB-IoT设备$IOTD_i$才能使用其私钥T_i生成合法签密并生成合法的聚合签名e_a。只有合法的AMF才能使用其私钥T_{AMF}解密数据,并通过使用每个NB-IoT设备$IOTD_i$的公钥A_i来验证聚合签名e_a。

[0049] 信令拥塞避免:在本发明的方法中,通过采用聚合签密方法,在设备组组长GROUP LEADER收到来自NB-IoT设备组的访问请求消息后,将大量签名Y_i转换为聚合签名e_a。然后,接入与移动性管理实体AMF将同时验证NB-IoT设备组,而无需每个NB-IoT设备进行单独验证。此过程可以大大减少信令开销并简化身份验证过程。另外,本发明的方法中的接入认证和数据传输过程是在不建立数据承载的情况下同时进行的,因此本发明的方法将大大减轻网络负担,避免网络拥塞。

[0050] 本发明所采用的基于格的同态加密技术具有简单的代数结构,并且涉及紧凑的并行计算以抵抗量子攻击,因此利用基于格的同态加密技术为大规模NB-IoT设备提出了快速认证与数据传输方法。本发明的方法可以同时实现接入认证和数据传输过程,并且与其他现有方案相比具有更好的效率,适用于未来5G网络中的NB-IoT系统。通过本发明的方法,具有相同属性或近距离的NB-IoT设备将形成NB-IoT设备组并选择设备组组长GROUP LEADER。当NB-IoT设备需要与5G网络通信时,每个NB-IoT设备都将签名和加密信息发送给设备组组长GROUP LEADER。之后,设备组组长GROUP LEADER聚合信息并将其发送到5G核心网络,以便5G核心网络可以验证NB-IoT设备组的合法性。

附图说明

[0051] 图1是本发明实施例提供的海量NB-IoT设备的抗量子快速认证与数据传输方法流程图。

[0052] 图2是本发明实施例提供的海量NB-IoT设备的抗量子快速认证与数据传输方法实现流程图。

具体实施方式

[0053] 为了使本发明的目的、技术方案及优点更加清楚明白,以下结合实施例,对本发明进行进一步详细说明。应当理解,此处所描述的具体实施例仅仅用以解释本发明,并不用于限定本发明。

[0054] 针对目前没有5G网络中针对海量NB-IoT设备的快速认证与数据传输的有效机制的问题。本发明大幅度减少接入认证与数据传输的信令开销和通信开销,优化了NB-IoT设备($IOTD_i$)和接入与移动性管理实体(AMF)之间的认证与数据传输延迟,实现5G网络中NB-IoT设备和目标AMF间的快速和安全的接入认证与数据传输。

[0055] 下面结合附图对本发明的应用原理作详细的描述。

[0056] 如图1所示，本发明实施例提供的海量NB-IoT设备的抗量子快速认证与数据传输方法包括以下步骤：

[0057] S101：SDN控制器中位于5G数据中心，认证切换模块AHM作为一种应用被放置于SDN控制器，用于监视和预测5G用户的位置和路径；在5G用户切换之前准备相关的基站或选择合适的基站从而确保无缝切换认证；

[0058] S102：5G用户控制自己的安全上下文信息并将其转移到目标基站BS本身；安全上下文信息可以直接用于用户和目标基站BS之间的相互认证。

[0059] 本发明实施例提供的5G网络中针对海量NB-IoT设备的抗量子快速认证与数据传输方法具体包括以下步骤：

[0060] 步骤一，系统初始化阶段；

[0061] 步骤二，基于群组的快速认证与数据传输阶段。

[0062] 在本发明的优选实施例中：系统初始化阶段具体包括：

[0063] (1)鉴权服务器AUSF首先计算系统参数$m=\lceil 6nlogq\rceil$与$l=O(\sqrt{nlogq})$，其中n为系统安全参数，q为系统安全参数n的多项式，符号$\lceil x\rceil$表示不大于x的整数，符号O(f(n))为关于系统安全参数n函数的复杂度；

[0064] (2)鉴权服务器AUSF设置聚合高斯参数$s_a \geq l\cdot\omega(\sqrt{logm})$，接入与移动性管理实体AMF高斯参数$s_{AMF}\geq l\cdot\omega(\sqrt{logm})$与窄带物联网NB-IoT设备高斯参数$s_i \geq l\cdot\omega(\sqrt{logm}), i=1,2...t$，其中t为NB-IoT设备数量，符号ω(f(m))为关于系统参数m函数的复杂度；同时鉴权服务器AUSF利用算法TrapGen(n,q,m)获得均匀随机矩阵A_a与基于矩阵A_a生成的格$\Lambda_q^{\perp}(A_a)$中的短基T_a，其中算法TrapGen(n,q,m)为多项式时间陷门生成算法。该算法输入参数为系统安全参数n，系统安全参数n的多项式q与系统参数m，该算法输出参数为均匀随机矩阵A_a与短基T_a；

[0065] (3)鉴权服务器AUSF设置t个格Λ_i以满足等式$\Lambda_1+\Lambda_2+...\Lambda_t=Z^m$和等式$\Lambda_1\cap\Lambda_2\cap...\cap\Lambda_t=\Lambda_q^{\perp}(A_a)$，其中$Z^m$为整数集上的n阶向量，符号∩为交集，$\Lambda_q^{\perp}(A_a)$为基于矩阵$A_a$生成的格；

[0066] (4)当NB-IoT设备$IOTD_i$接入5G网络时，5G接入与移动性管理实体AMF对每个设备$IOTD_i$通过执行认证与密钥协商协议5GAKA或EAPAKA'以完成初始认证；

[0067] (5)在成功完成初始认证后，鉴权服务器AUSF利用算法TrapGen(n,q,m)为每个NB-IoT设备$IOTD_i$生成一个公钥/私钥对(A_i,T_i)并安全地分配给每个NB-IoT设备$IOTD_i$，其中算法TrapGen(n,q,m)为多项式时间算法，公钥A_i为均匀随机矩阵，私钥T_i为基于矩阵A_i生成的格$\Lambda_q^{\perp}(A_i)$中的短基T_i；

[0068] (6)在成功完成初始认证后，鉴权服务器AUSF利用算法TrapGen(n,q,m)为每个接入与移动性管理实体AMF生成一个公钥/私钥对(A_{AMF},T_{AMF})并安全地分配给每个接入与移动性管理实体AMF，其中算法TrapGen(n,q,m)为多项式时间算法，公钥A_{AMF}为均匀随机矩阵，私钥T_{AMF}为基于矩阵A_{AMF}生成的格$\Lambda_q^{\perp}(A_{AMF})$中的短基$T_{AMF}$。

[0069] 在本发明的优选实施例中：基于群组的快速认证与数据传输阶段具体包括：

[0070] (1)每个NB-IoT设备$IOTD_i$准备其将要发送的明文数据向量$U_i = PDU_i \| ID_{IOTD_i} \| GID = (U_1, ..., U_m)^T$，其中$PDU_i$为协议数据单元，$ID_{IOTD_i}$为NB-IoT设备的身份，GID为NB-IoT设备群组的身份；然后每个NB-IoT设备$IOTD_i$利用目标接入与移动性管理实体AMF的公钥A_{AMF}计算密文$C_i = A_{AMF} * U_i$；同时每个NB-IoT设备$IOTD_i$利用多项式时间算法SamplePre与自身私钥T_i生成签名$Y_i = (e_i, x_i)$，其中$e_i = SamplePre(A_i, T_i, H_1(x_i), s_i)$为算法SamplePre输出结果，$x_i$为随机数，$H_1$为哈希函数，$s_i$为高斯参数；每个NB-IoT设备$ID_{IOTD_i}$构造一个接入请求信息将$(C_i, Y_i)$发送给设备组组长GROUP LEADER；

[0071] (2)设备组组长GROUP LEADER在成功接收到组内所有NB-IoT设备的接入请求后执行以下步骤：

[0072] a)利用每个NB-IoT设备的部分签名e_i与t个格Λ_i计算部分聚合签名$e = e_1 \bmod \Lambda_1$，$e = e_2 \bmod \Lambda_2, \cdots, e = e_t \bmod \Lambda_t$；

[0073] b)利用多项式时间算法SampleGaussian计算部分聚合签名$e_0 = SampleGaussian(T_a, s_a, -e)$，其中$T_a$为基于矩阵$A_a$生成的格$\Lambda_q^{\perp}(A_a)$中的短基，$s_a$为高斯参数，e为部分聚合签名；

[0074] c)利用上述步骤计算出的部分聚合签名e，e_0计算聚合签名$e_a = e_0 + e$；

[0075] d)构造一个聚合接入请求信息将$(e_a, \{C_i, x_i\}_{i=1}^t)$发送给5G网络中的目标接入与移动性管理实体AMF，其中e_a为聚合签名，C_i为每个NB-IoT设备生成的密文，x_i为每个NB-IoT设备生成的随机数；

[0076] (3)接入与移动性管理实体AMF在成功接收到设备组组长发送的聚合接入请求后执行以下步骤：

[0077] a)验证聚合签名e_a是否合法，验证公式为下述公式(A)与公式(B)：

[0078] $$\| e_a \| \leq s_a \sqrt{m} \qquad (A)$$

[0079] $H_2(H_1(x_1), H_1(x_2) \ldots H_1(x_t))$

[0080] $= H_2(A_1(e_a \bmod \Lambda_1) \bmod q, \ldots, A_t(e_a \bmod \Lambda_t) \bmod q)$ (B)

[0081] 其中e_a为聚合签名，s_a为高斯参数，m，q为系统参数，H_1，H_2为哈希函数，x_i为NB-IoT设备生成的随机数，A_i为均匀随机矩阵，Λ_i为格；

[0082] b)若上述聚合签名是合法的，接入与移动性管理实体AMF利用多项式时间算法SamplePre与自身私钥T_{AMF}解密出每个NB-IoT发送的明文数据$U_i = SamplePre(A_{AMF}, T_{AMF}, C_i, s_{AMF})$，其中$A_{AMF}$为接入与移动性管理实体AMF的公钥，$C_i$为密文，$s_{AMF}$为高斯参数；同时生成一个随机的认证成功标识符Succ；

[0083] c)利用多项式时间算法SamplePre与自身私钥T_{AMF}生成签名$Y_{AMF} = SamplePre(A_{AMF}, T_{AMF}, H_1(Succ), s_{AMF})$，其中$A_{AMF}$为AMF的公钥，$H_1$为哈希函数，$s_{AMF}$为高斯参数；

[0084] d)若此时AMF有需要发送的下行数据，则利用每个NB-IoT设备的公钥A_i加密下行数据密文$C_{AMF} = A_i * PDU_{AMF}$，其中$PDU_{AMF}$为协议数据单元；

[0085] e)构造一个聚合接入响应信息将$(ID_{AMF}, Y_{AMF}, C_{AMF}, Succ)$发送给目标设备组组长GROUP LEADER，其中ID_{AMF}为AMF的身份，Y_{AMF}为AMF生成的签名，C_{AMF}为下行数据密文，Succ为认证成功标识符；

[0086] (4)目标设备组组长GROUP LEADER在成功接收到聚合接入响应信息后将接入响应

信息发分发到小组内每个目标NB-IoT设备；

[0087] (5)小组内每个目标NB-IoT设备在成功接收到接入认证响应信息后执行以下步骤：

[0088] a)验证AMF生成的签名Y_{AMF}是否合法，验证公式为下述公式(C)与公式(D)：

[0089] $A_{AMF}Y_{AMF}=H_1(Succ)$ (C)

[0090] $$\| Y_{AMF} \| \leq s_{AMF}\sqrt{m} \qquad (D)$$

[0091] 其中A_{AMF}为AMF的公钥，$H_1(Succ)$为经过哈希函数H_1计算的成功标识符，s_{AMF}为高斯参数，m为系统参数；

[0092] b)若上述AMF的签名Y_{AMF}是合法的，则利用多项式时间算法SamplePre与自身私钥T_i解密下行数据密文C_{AMF}从而获得下行数据明文$PDU_{AMF}=SamplePre(A_i,T_i,C_{AMF},s_i)$，其中$A_i$为每个NB-IoT设备的公钥，$s_i$为高斯参数。

[0093] 下面结合对比对本发明的应用效果作详细的描述。

[0094] 对比文件1J.Cao,M.Ma,H.Li,“GBAAM:group-based access authentication for MTC in LTE networks,”Security and Communication Networks,Vol.8,No.17,2015,pp.3282-3299.

[0095] 对比文件2J.Li,M.Wen,and T.Zhang,“Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A Networks,”IEEE Internet ofThings Journal,Vol.3,No.3,2016,pp.408-417.

[0096] 对比文件3C.Lai,H.Li,R.Lu,R.Jiang,X.Shen,“LGTH:A lightweight group authentication protocol for machine-type communication in LTE networks,”Proceedings of IEEE Global Communications Conference(GLOBECOM'13),GA,USA,2013,pp.832-837.

[0097] 对比文件4Y.W.Chen,J.T.Wang,K.H.Chi,and C.C.Tseng,“Group-Based Authentication and Key Agreement,”Wireless Personal Communications,Vol.62,No.4,2010,pp.1-15.

[0098] 对比文件5Y.Zhang,J Chen,H Li,W Zhang,J.Cao,C Lai,“Dynamic group based authentication protocol for machine type communications,”Intelligent Networking and Collaborative Systems(INCoS),Bucharest,2012,pp.334-341.

[0099] 对比文件6C.Lai,H.Li,X.Li,and J.Cao,“A novel group access authentication and key agreement protocol for machine-type communication,”Transactions on Emerging Telecommunications Technologies,Vol.26,No.3,2015,pp.414-431.

[0100] 对比文件7C.Lai,H.Li,R.Lu,X.Shen,“SE-AKA:A secure and efficient group authentication and key agreement protocol for LTE networks,”Computer Networks,Vol.57,No.17,2013,pp.3492-3510.

[0101] 对比文件8R.Jiang,C.Lai,J.Luo,X.Wang,and H.Wang,“EAP-Based Group Authentication and Key Agreement Protocol for Machine-Type Communications,”International Journal of Distributed Sensor Networks,vol.2013,Article ID 304601,2013.

[0102] 对比文件9J.Cao,P.Yu,M.Ma,W.Gao,``Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network,"IEEE Internet ofThings Journal,2018,accepted.

[0103] 本发明的发明与现有方案相比如下表所示：

[0104]

方案 / 性质	1	2	3	4	5	6	7	8	9	本发明
相互认证	是	是	是	是	是	是	是	是	是	是
会话密钥建立	是	是	是	是	是	是	是	是	是	是
承受协议攻击(包括量子攻击)	否	否	否	否	否	否	否	否	否	是
普适性（可扩展性）	否	否	否	否	否	否	否	否	是	是
用户匿名性和不可链接性	是	否	否	是	否	是	否	否	是	是
通信开销	高	高	高	高	高	高	高	高	低	低
计算开销	高	低	低	低	低	低	低	低	高	低

[0105] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

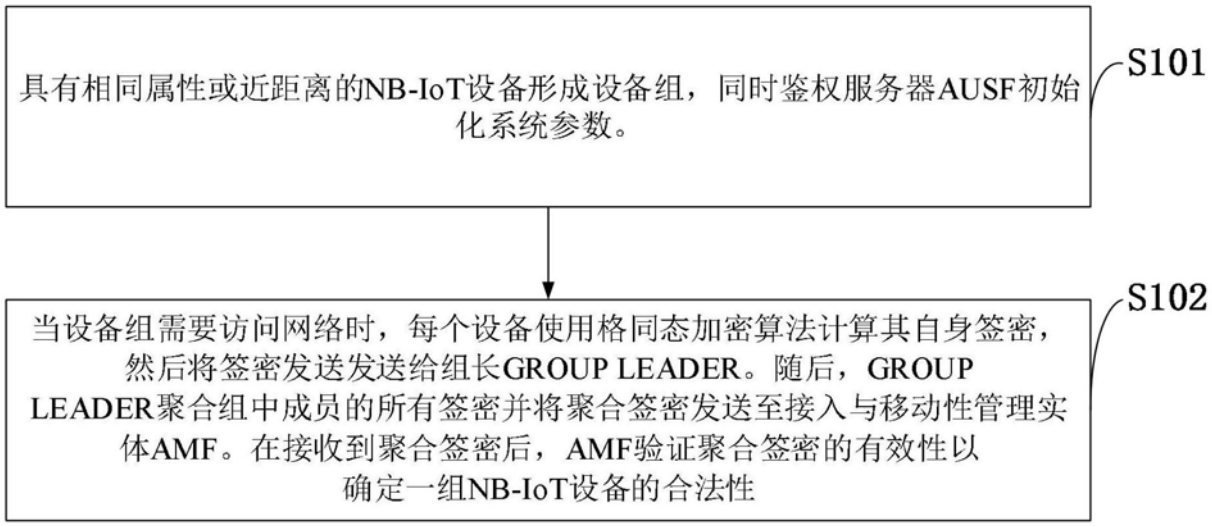

具有相同属性或近距离的NB-IoT设备形成设备组，同时鉴权服务器AUSF初始化系统参数。
S101
当设备组需要访问网络时，每个设备使用格同态加密算法计算其自身签密，然后将签密发送发送给组长GROUP LEADER。随后，GROUP LEADER聚合组中成员的所有签密并将聚合签密发送至接入与移动性管理实体AMF。在接收到聚合签密后，AMF验证聚合签密的有效性以确定一组NB-IoT设备的合法性
S102

图1

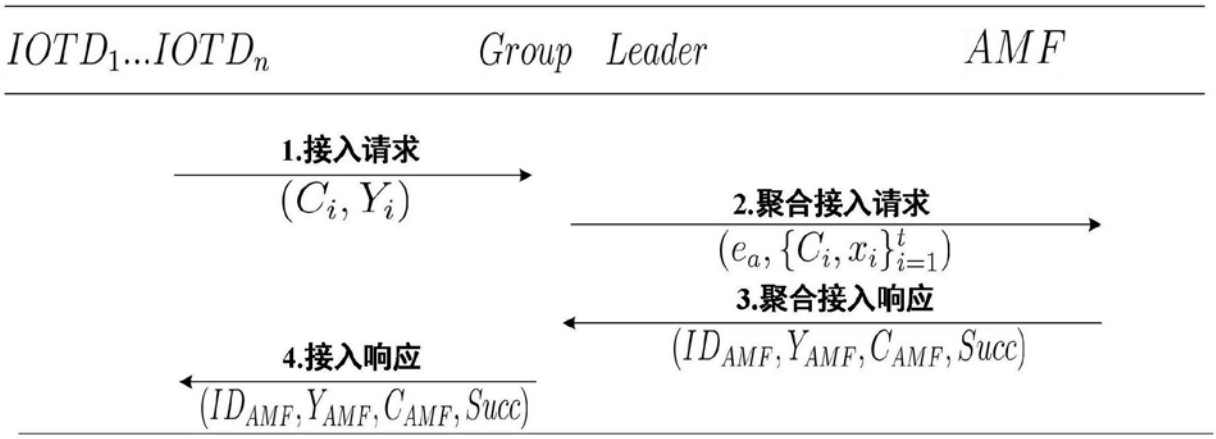

$IOTD_1 ... IOTD_n$
Group Leader
AMF
1.接入请求
(C_i, Y_i)
2.聚合接入请求
$(e_a, \{C_i, x_i\}_{i=1}^{t})$
3.聚合接入响应
$(ID_{AMF}, Y_{AMF}, C_{AMF}, Succ)$
4.接入响应
$(ID_{AMF}, Y_{AMF}, C_{AMF}, Succ)$

图2