低开销的 NB-IoT 节点群组身份安全认证协议

常相茂[1]，占俊[1]，王志伟[2]

（1. 南京航空航天大学计算机科学与技术学院，江苏 南京 211106；
2. 南京邮电大学计算机学院、软件学院、网络空间安全学院，江苏 南京 210023）

摘 要：针对现有 NB-IoT 网络的安全认证协议在大规模接入请求认证时会产生大量信令的问题，提出了一种基于 Schnorr 聚合签名和中国剩余定理的群组身份安全认证协议。该协议使服务器能够使用固定大小的信令对节点群组进行一次性认证，采用基于中国剩余定理的会话密钥分发机制，使服务器可以用固定大小的数据完成对群组中节点的密钥派发。安全验证和性能分析结果表明，所提协议具有可靠的安全性能，且在传输开销和带宽消耗方面表现优异。

关键词：群组身份安全认证协议；中国剩余定理；聚合签名；窄带物联网

中图分类号：TP393.2

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021228

Low-cost group-based identity security authentication protocol for NB-IoT nodes

CHANG Xiangmao[1], ZHAN Jun[1], WANG Zhiwei[2]

1. School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
2. School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Abstract: To address the problem of huge number of signaling requests when large-scale devices request authentication in NB-IoT network, a low-cost group identity security authentication protocol based on Schnorr aggregate signature and Chinese reminder theorem was proposed. The protocol enabled the server to perform one-time authentication of the device group with a size-fixed group authentication request, which effectively reduced the bandwidth consumption of the authentication request. The protocol used a session key distribution mechanism based on the Chinese remaining theorem, allowing the server to complete the distribution of keys for each device in the group by size-fixed message. The results of security verification and the performance analysis show that the proposed protocol has reliable safety and superior performance in terms of transmission load and bandwidth consumption.

Keywords: group-based identity security authentication protocol, Chinese remainder theorem, aggregate signature, NB-IoT

1 引言

随着物联网应用的普及和发展，许多由通信引起的问题逐渐凸显出来，例如应用场景分散、行业标准过多以及通信能耗过高等。为解决这些问题，2016 年，全球第三代合作伙伴计划（3GPP, 3rd generation partnership project）委员会克服各种技术困难最终制定了窄带物联网（NB-IoT, narrowband Internet of things）的核心标准[1]。同传统的无线物联网通信技术相比，NB-IoT 具有大容量、广覆盖、低功耗和低成本特点[2]，这为部署在长期难以达到的地方且传输数据量较少的物联网设备提供了一种更好的网络接入方式，已经被广泛用于智能停车[3]、智能抄表[4]和智能医院[5]等场景。随着 NB-IoT 技术逐渐融入人们的生活，越来越多的 NB-IoT 节点设备连接到网络，来满足用户多样化的需求。但是由于

收稿日期：2021−08−24；**修回日期**：2021−11−24
基金项目：国家自然科学基金资助项目（No.61672282）
Foundation Item: The National Natural Science Foundation of China (No.61672282)

设备资源受限、位置暴露，这些 NB-IoT 节点极易遭受攻击者的攻击，尤其是那些用于收集和传输用户敏感数据的设备。一旦这些设备遭受攻击，就会导致用户敏感数据遭到泄露，造成不可挽回的损失。因此，在访问认证过程和数据传输过程中，对用户身份隐私和传输数据安全的保障至关重要。

NB-IoT 网络消耗大约 180 kHz 的带宽，上下行峰值速率理论上不会超过 250 kbit/s[2]，因此当大规模的 NB-IoT 节点激活向核心服务器申请接入认证时，大量的信令请求会增加网络的通信压力，甚至引起通信堵塞，从而影响 NB-IoT 应用程序的服务质量，降低系统运行效率。随机时延机制是一种常用的避免数据冲突和网络拥塞的方法，即当 NB-IoT 节点被唤醒后，各自随机延迟一段时间再进行接入以免并发通信造成冲突，然而该机制存在如下 2 个方面的弊端：一是该机制并没有减少所需认证消息的数量，当存在大量 NB-IoT 节点需要与服务器进行认证时（每个 NB-IoT 小区可达 5 万连接数[1]），需要非常大的时延来避免冲突；二是该机制无法确保避免冲突，依然存在 2 个或多个节点延迟相同时间而发生并发冲突的情况。为提高大规模节点接入认证时的效率、降低通信开销，许多基于群组的聚合认证协议被提出[6]。将同一区域内的节点根据功能或其他相似特性划分为一组，认证时服务器对群组的身份进行验证，从而一次性完成对群组中所有成员身份的认证。然而，现有协议中群组认证请求的数据大小会随群组中成员数量的增加而变大，当规模庞大的 NB-IoT 节点群组申请认证时，仍有可能会引起通信堵塞。

本文基于 Schnorr 聚合签名技术实现 NB-IoT 节点群组的聚合签名，将群组的认证请求大小设置为固定值，不会随着群组中成员数量的变化而变化，同时，为了保障数据通信的安全，采用基于中国剩余定理的密钥分发管理机制，服务器能以固定的信息量完成对群组内成员会话密钥信息的分发，因此服务器回复消息是一个定值。将群组和服务器认证时的通信量固定为确定的大小，从而有效减少带宽消耗，降低堵塞风险。性能分析结果表明，与现有身份安全认证协议相比，本文所提协议在传输开销和带宽消耗方面表现优异。本文有以下两点贡献。

1) 本文基于 Schnorr 聚合签名和中国剩余定理提出了一种新型的群组身份安全认证协议，可以实现服务器和 NB-IoT 节点的双向认证，认证产生的通信量不随群组规模的增大而增加，解决大规模 NB-IoT 节点安全认证时效率低下和占用大量带宽资源的问题。

2) 本文使用协议形式化分析工具 Scyther 对协议的安全性进行仿真分析，验证了所提协议能够提供可靠的安全性能，可抵御重放攻击、中间人攻击等常见协议攻击模式。

2　相关工作

NB-IoT 是一种蜂窝网络，在传统的蜂窝网络 LTE-A（long term evolution-advanced）中，基于群组的身份安全认证协议主要可分为两类。在第一类身份认证协议中，设备组由属于同一归属网络中的用户设备（UE, user equipment）或者机器类型通信设备（MTCD, machine type communication device）组成。当设备组中第一个成员移动进入服务网络的覆盖范围后，该成员在执行认证过程中会将整个群组的相关信息发送给网络。Chen 等[6]首先提出了该类型的群组身份安全认证协议，用于大规模设备从归属网络漫游到服务网络的访问控制，随后其他研究人员也提出了一些类似的协议[7-10]。在该类方案中，服务网络对第一个群组设备进行认证后，可以简化同其他成员的认证过程，从而减少服务网络和归属网络之间的通信开销。但是，群组中每个设备仍然需要单独向服务网络发起访问认证请求，这依旧会导致大量的信令开销，无法避免通信堵塞。

在第二类身份认证协议中，设备群组会选择一个设备作为群组组长 Leader，由 Leader 聚合并发送群组成员的认证请求。当设备群组进行访问身份认证时，Leader 将收集群组中所有成员的身份认证请求并聚合为一条群组身份认证请求，而服务端只需要验证 Leader 发送的聚合身份认证请求就可以验证设备组中所有成员的身份。Lai 等[11]提出了一种基于聚合消息认证码的轻量级群组访问认证协议。之后，Cao 等[12]提出了一种利用双线性配对聚合签名技术的群组身份认证协议。Li 等[13]采用(t, m, n)密钥共享机制和 Diffie-Hellman 密钥交换协议提出了一种具有动态更新策略的群组身份安全认证协议。为了解决公钥体系中的密钥托管问题，Lai 等[14]提出了一种基于无证书聚合签名技术的聚合认证协议，来提高大规模 MTCD 访问 3GPP 网络的效率和安全性。但是，无证书聚合签名技术中所使用的双线性配对操作会导致大量的计算负载，并不适用

于资源受限的物联网设备。为了降低计算负载，Lai 等[15]提出了一种仅使用哈希函数和异或操作的轻量级聚合身份认证机制。Ren 等[16]提出了一种基于物理不可克隆函数（PUF, physical unclonable function）的双向认证。PUF 用于生成共享根密钥，群组 Leader 负责聚合和中转认证信息，通过激活海量设备的附着请求消息达到降低信令和通信开销的目的。与之不同，本文通过 Schnorr 聚合签名和中国剩余定理减少认证消息来降低通信开销。

在 NB-IoT 网络中，Cao 等[17]使用不基于双线性配对的无证书签密技术提出了一种群组聚合访问认证协议，以实现大规模 NB-IoT 设备的快速认证和数据传输。Zhang 等[18]提出了一种基于无证书签名技术的多方快速认证机制，该机制实现了 NB-IoT 网络中多个 UE 以及认证服务器之间的快速认证。为了抵御量子攻击的威胁，Yu 等[19-20]提出了一种基于格加密的抗量子攻击聚合身份认证协议，但是其计算负载较高，并不适于资源受限的 NB-IoT 设备。尽管这些协议通过聚合认证请求减少了认证期间的通信数据量，但是聚合请求的大小仍然受组中成员数量的影响，当设备组中成员数量很大时，仍然存在通信阻塞的风险。

Schnorr 签名算法因为可靠的安全性、可聚合的特点，已经被广泛应用于各种安全认证领域。Maxwell 等[21]基于 Schnorr 算法提出了一种多重签名算法 Musig，用于提高比特币中合法性验证的效率，增强用户隐私保护。Ni 等[22]使用 Schnorr 算法提出了一种支持 5G 网络切片和雾计算的匿名身份安全认证协议，但是协议建立在网络资源充裕的情况下，并不适于网络资源有限的 NB-IoT 网络。中国剩余定理可以将分发的信息进行聚合，实现轻量化的组密钥管理机制，Vijayakumar 等[23]基于此提出了一种轻量化的、集中式的群组密钥管理机制，用于多播安全通信，之后在无线传感网络、车联网等物联网环境中也得到了进一步的应用[24-26]。但是这些协议只考虑成员节点数量有限的情况，并未考虑大规模数量节点情况对网络可能造成的巨大压力。

3 预备知识

3.1 椭圆曲线离散对数难题

假设 p 是一个大素数，E 是有限域 F_p 上的椭圆曲线，$G \in E(F_p)$ 是椭圆曲线上的一个 q 阶点。椭圆曲线离散对数难题是给定 $Q \in E(F_p)$ 和 G，求解整数 $k \in Z_q^*$ 使等式 $Q = kG$ 成立。可以证明给定 G 和 k 求解 Q 非常容易，但是给定 Q 和 G 求解 k 非常困难，目前还没有一个有效的方法可以解决该难题[27]。

3.2 Schnorr 聚合签名

Schnorr 签名算法最初由德国的数学家、密码学家 Schnorr[28]提出，在性能、安全、体积、扩展性等诸多方面都优于椭圆曲线数字签名算法。Schnorr 签名算法的安全性可以通过随机预言模型进行验证[29]，而且由于算法是线性的，因此可以进行聚合签名或者对大规模的签名进行一次性的验证，有效节省空间、提高效率。

Schnorr 签名的生成过程为给定大素数 p、椭圆曲线 $E(F_p)$ 和椭圆曲线上的 q 阶点 $G \in E(F_p)$，选择随机数 $r \in Z_q^*$ 并计算 $R = rG$。使用私钥 $x \in Z_q^*$ 对消息 m 进行签名，Schnorr 签名为 (R,s)，其中，s 如式(1)所示[30]。

$$s = r + \text{hash}\left(X \| R \| m\right)x \tag{1}$$

使用公钥 $X = xG$ 对消息 m 签名有效性的验证如式(2)所示。

$$sG = R + \text{hash}\left(X \| R \| m\right)X \tag{2}$$

Schnorr 的聚合签名是使用多个私钥对消息进行聚合签名，验证时使用由多个私钥派生出的公共公钥进行验证。例如使用私钥 $x_1, x_2 \in Z_q^*$ 对消息 m 聚合签名，选择 $r_1, r_2 \in Z_q^*$ 并分别计算 s_1, s_2，公共公钥为 $X = (x_1 + x_2)G$，聚合签名 (R,s) 为

$$\begin{cases} R = R_1 + R_2 = r_1G + r_2G \\ s_1 = r_1 + \text{hash}\left(X \| R \| m\right)x_1 \\ s_2 = r_2 + \text{hash}\left(X \| R \| m\right)x_2 \\ s = s_1 + s_2 \end{cases} \tag{3}$$

聚合签名的验证使用公共公钥，验证过程与单个签名的验证相同，如式(2)所示。

3.3 中国剩余定理

中国剩余定理又称孙子定理，是数论中的一个重要定理，该定理给出了一元线性同余方程组的有解判定条件和有解情况下的解的具体形式。给定两两互质的正整数 $m_1, m_2, \cdots, m_n$ 和任意正整数 $a_1, a_2, \cdots, a_k$，如式(4)所示的同余方程组有解，且在

$M = m_1 m_2 \cdots m_n$ 模下有唯一解。

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\ m_1) \\ x \equiv a_2 (\mathrm{mod}\ m_2) \\ \quad \vdots \\ x \equiv a_n (\mathrm{mod}\ m_n) \end{cases} \tag{4}$$

对所有 $i = 1,2,\cdots,n$，计算 $M_i = M / m_i$ 和模乘逆 M_i^{-1} 满足式(5)。

$$M_i M_i^{-1} \equiv 1 (\mathrm{mod}\ m_i) \tag{5}$$

方程组的唯一解如式(6)所示。

$$x \equiv \sum_{i=1}^{n} a_i M_i M_i^{-1} (\mathrm{mod} M) \tag{6}$$

如果将 m_i 看作节点私钥，a_i 看作需要分发的信息，那么服务器只需要求解并广播 x 就可以完成对 n 条信息 $a_1, a_2, \cdots, a_n$ 的分发，节点可以使用私钥 m_i 通过求模运算得到消息 $a_i \equiv x (\mathrm{mod}\ m_i)$。

4　系统模型

本文讨论的 NB-IoT 网络系统结构如图 1 所示。同一区域内的 NB-IoT 节点根据功能或其他相似特性划分为一组，同一节点群组中成员属于同一应用服务器，会根据节点计算能力、电池容量等情况选择一个节点作为群组 Leader。群组中的 NB-IoT 节点会在同一时刻唤起，通过 NB-IoT 网络与应用服务器进行通信。节点发送或接收数据前，服务器需要对节点的身份进行安全认证。服务器会生成认证过程中所使用的所有密钥，同时扮演密钥生成中心的角色。

在本文所讨论的系统中，NB-IoT 节点与服务器之间的通信是不安全的，外部攻击者可以控制、截取或者篡改NB-IoT节点与服务器的无线通信消息。除此之外，攻击者还可以模仿伪装成应用服务器或者 NB-IoT 节点，进行重放攻击、中间人攻击等攻击，实现上传错误数据或者盗取隐私数据。由于 NB-IoT 节点数量巨大，同时与服务器进行通信时，大量的信令可能会导致网络负担过重或通信堵塞。为了同时满足 NB-IoT 网络对认证效率、安全性和通信量限制的要求，本文所提协议需要满足以下几点要求。

1) 双向认证。当节点群组与服务器建立连接时，服务器需要完成对节点群组中所有节点的身份认证。除此之外，节点群组中的所有成员也能够对服务器的身份进行安全认证。

2) 会话密钥建立。在认证的过程中，能够对用于后续服务器与节点通信的会话密钥进行更新，以保护后续传输数据的安全性。

3) 对常见协议攻击的抗性。协议需要能够抵御常见的一些攻击，例如重放攻击、中间人攻击、伪装攻击等。

4) 高效性。服务器能够一次性完成对这个节点群组成员的身份认证，同时应降低通信和计算负载，来避免通信堵塞。

5　安全认证协议

本节所使用的符号定义如表 1 所示。

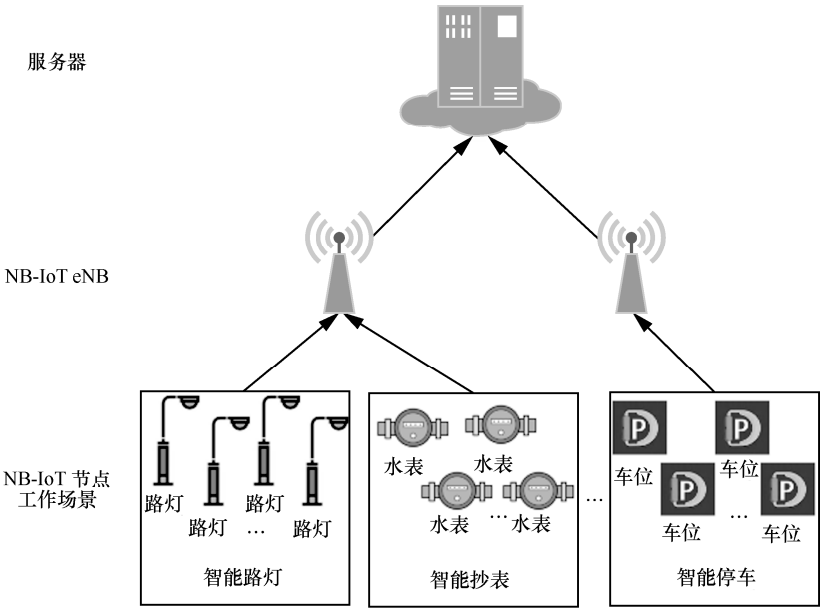


图 1　NB-IoT 网络系统结构

表 1 符号定义

符号	定义
UE_i	群组中第 i 个用户节点
$\mathrm{ID}_i, \mathrm{GID}$	UE_i 、群组的身份标识
p, q	大素数
$E(F_p)$	在有限域 F_p 上的椭圆曲线
G	$E(F_p)$ 上的 q 阶点
x_i, x_c	UE_i 、服务器的私钥
P_i, P, P_c	UE_i 、群组和服务器的公钥
g_k	群组的组密钥
L	群组的公共参数
s_i, s, s_c	UE_i 、群组和服务器的签名
T_u, T_c	群组和服务器的当前时间戳
hash()	防碰撞单项哈希函数
$\|\|$	字符串连接操作
SK_i	UE_i 和服务器的会话密钥

5.1 初始化阶段

在初始化阶段，服务器根据所选择的安全等级参数，生成认证所需的各种参数以及服务器自身的密钥。服务器首先决定安全等级参数 k，并选择一个大素数 $p > 2^k$。然后在有限域 F_p 上选择椭圆曲线 $E(F_p)$，$E(F_p)$ 上的 q 阶点 $G \in E(F_p)$ 和哈希函数 $\mathrm{hash}(): \{0,1\}^* \to Z_q^*$。最后选择随机数 $x_c \in Z_q^*$ 作为自身的私钥，计算公钥 $P_c = x_c G$，将 $\{q, E(F_p), G, \mathrm{hash}(), P_c\}$ 作为系统参数公布并保密 x_c。

5.2 注册阶段

在注册阶段，节点 UE_i 向服务器进行注册获得密钥以及所在群组的相关参数。

假设群组由 n 个节点组成，UE_i 向服务器发送自身 ID_i 进行注册，服务器进行以下步骤。

1) 选择随机数 $x_i \in Z_q^*$ 作为 UE_i 私钥，同一群组中节点的私钥应该两两互质。之后服务器计算节点公钥 $P_i = x_i G$。

2) 计算 $M = x_1 x_2 \cdots x_n$ 和 $M_i = M / x_i$。

3) 计算 M_i 在模 x_i 下的模乘逆 $M_i M_i^{-1} \equiv 1 (\mathrm{mod}\ x_i)$，之后计算 $\mathrm{var}_i = M_i M_i^{-1}$。

4) 随机选择群组的身份标识 $\mathrm{GID} \in Z_q^*$ 和群组密钥 $g_k \in Z_{q/4}^*$，群组密钥 g_k 应该小于群组中所有私钥 x_i [23]。之后服务器计算 $\mathrm{GK} = g_k \sum_{i=1}^{n} \mathrm{var}_i$ 用于向群组中成员分发组密钥，UE_i 可以通过 $g_k \equiv \mathrm{GK} (\mathrm{mod}\ x_i)$ 来解密获得组密钥。

5) 为了抵抗恶意密钥攻击[21]，采用非线性的方式来生成群组的公共公钥 $P = \sum_{i=1}^{n} [\mathrm{hash}(L \| P_i) P_i]$，其中公共参数 $L = \mathrm{hash}(g_k \| P_1 \| P_2 \| \cdots \| P_n)$。

6) 最后，服务器生成 $\{x_i, P_i, \mathrm{GID}, \mathrm{GK}, L, P\}$，并将其预先安装到 UE_i 或通过安全信道发送给 UE_i，并保存 $\{\mathrm{ID}_i, \mathrm{var}_i, \mathrm{GID}, g_k, P\}$。

5.3 双向认证阶段

在双向认证阶段，群组中节点完成同服务器的双向认证以及会话密钥分发。当群组唤醒准备同服务器发送或接收数据时，所有节点对当前时间戳进行签名并由群组 Leader 聚合发送给服务器进行认证，服务器根据聚合签名的有效性可以对整个群组进行一次性认证。由于群组内节点数量有限，在群组 Leader 聚合每个节点的签名时，Leader 可以给每个节点分配不同的子载波避免冲突和信道阻塞。

为了保证后续通信的安全，服务器为每个节点选择随机数用于生成会话密钥。服务器利用中国剩余定理加密保护随机数，签名后发送给群组 Leader，群组 Leader 再分发给节点。在验证了服务器签名的有效性后，节点使用私钥解密得到随机数，生成会话密钥。

1) UE_i 随机选择 $r_i \in Z_q^*$ 并计算 $R_i = r_i G$，之后将 R_i 发送给 Leader。

2) Leader 收集群组内所有 UE_i 的 R_i 后，计算 $R = \sum_{i=1}^{n} R_i$。之后 Leader 将时间戳 T_u 和 R 发送给 UE_i。

3) UE_i 根据自己的当前时刻与 T_u 的差异检查时间戳 T_u 的时效性，计算签名 $s_i = r_i + \mathrm{hash}(T_u \| R \| P) \cdot \mathrm{hash}(L \| P_i) x_i$。之后 UE_i 将 s_i 发送给 Leader。

4) Leader 收集群组内所有 UE_i 的签名 s_i 后，计算聚合签名 $s = \sum_{i=1}^{n} s_i$。最后 Leader 将 $\{\mathrm{GID}, T_u, R, s\}$ 发送给服务器请求认证。

5) 服务器接收到群组的认证请求后，执行以下步骤。

① 根据自己的当前时刻与 T_u 的差异检查时间戳 T_u 的时效性。

② 通过计算 $sG = R + \mathrm{hash}(T_u \| R \| P) P$ 是否成立来验证聚合签名的有效性，具体过程如式(7)所示。

$$sG=\sum_{i=1}^{n}s_iG=$$

$$\sum_{i=1}^{n}[r_i+\text{hash}(T_u\|R\|P)\text{hash}(L\|P_i)x_i]G=$$

$$\sum_{i=1}^{n}r_iG+\text{hash}(T_u\|R\|P)\sum_{i=1}^{n}[\text{hash}(L\|P_i)P_i]=$$

$$R+\text{hash}(T_u\|R\|P)P \tag{7}$$

③ 随机选择 $k_i\in Z_{q/4}^*$ 用于生成和 UE_i 的会话密钥 $\text{SK}_i=\text{hash}(\text{ID}_i\|T_u\|T_c\|k_i\|g_k)$。

④ 计算 $K=\sum_{i=1}^{n}(k_i\text{var}_i)$。

⑤ 选择随机数 $r_c\in Z_q^*$ 并计算 $R_c=r_cG$。

⑥ 对时间戳 T_c 和 K 签名，计算 $s_c=r_c+\text{hash}(K\|T_c\|R_c\|P_c\|g_k)x_c$。

⑦ 将 $\{K,T_c,R_c,s_c\}$ 发送给 Leader。

6) Leader 将收到的服务器回复消息广播给所有节点。

7) UE_i 接收到回复消息后，执行以下步骤。

①验证时间戳 T_c 的时效性。

②验证服务器签名 s_c 的有效性，过程如式(8)所示。

$$s_cG=r_cG+\text{hash}(K\|T_c\|R_c\|P_c\|g_k)(x_cG)=$$
$$R_c+\text{hash}(K\|T_c\|R_c\|P_c\|g_k)P_c \tag{8}$$

③解密随机数 $k_i\equiv K(\text{mod}\ x_i)$。

④计算会话密钥 $\text{SK}_i=\text{hash}(\text{ID}_i\|T_u\|T_c\|k_i\|g_k)$。

整个认证过程如算法 1 所示。

算法 1　NB-IoT 节点群组身份安全认证协议

输入　群组内 N 个 NB-IoT 节点的 ID，服务器安全等级 k，大于 2^k 的素数 p，椭圆 $E(F_p)$ 上的 q 阶点 $G\in E(F_p)$ 和哈希函数 $\text{hash}():\{0,1\}^*$

输出　认证成功与否

1) 服务器根据 $E(F_p)$ 性质与 hash() 产生随机数集合 Z_q^*，选取私钥 $x_c\in Z_q^*$，计算公钥 $P_c\leftarrow x_cG$，公布 $\{q,E(F_p),G,\text{hash}(),P_c\}$，保密 x_c

2) 服务器为每个 UE_i 选取私钥 x_i，根据每个 UE_i 的 ID 计算其公钥 P_i，将 $\{x_i,P_i,\text{GID},\text{GK},L,P\}$ 预装或通过加密信道传给每个 UE_i（其中 GID 是群组 ID）

3) 所有 UE 的公钥在 Leader 处聚合为 R，Leader 将时间戳 T_u 与 R 发回每个 UE_i

4) 每个 UE_i 核验 T_u 的时效性后计算签名，所有 UE 的签名在 Leader 处聚合为 s

5) Leader 发送 $\{\text{GID},T_u,R,s\}$ 给服务器请求认证

6) if (T_u 有效&& $sG==R+\text{hash}(T_u\|R\|P)P$)

7) 计算 SK_i、服务器的私钥 r_c、公钥 R_c 和 K，计算 K 和 T_c 的签名 s_c

8) 服务器发送 $\{K,T_c,R_c,s_c\}$ 至 Leader

9) Leader 将 $\{K,T_c,R_c,s_c\}$ 广播给每个 UE_i 进行认证

10) if($s_cG=R_c+\text{hash}(K\|T_c\|R_c\|P_c\|g_k)P_c$ && T_c 有效)

11) return 认证成功

12) end if

13) return 认证失败

14) end if

5.4　组密钥更新阶段

群组中的节点可能因为应用需求改变或发生故障等原因退出群组，附近节点也可能因为应用需求变化使唤醒时间变动，从而需要加入群组。在本文协议中，组密钥可用于生成群组公共公钥、会话密钥以及认证服务器，还可用于在组内建立安全通信和加密服务器发送给群组的分发消息。因此，当组成员发生变动时，应及时更新组密钥，以避免可能存在的安全隐患，保证群组认证和通信的安全。

5.4.1　组成员离开

当组成员 UE_{old} 离开群组时，服务器执行以下操作更新组密钥 $g_{k_{\text{new}}}$。

1) 服务器选择随机数 $g_{k_{\text{new}}}\in Z_{q/4}^*$ 作为新的组密钥。

2) 计算 $\text{GK}_{\text{new}}=g_{k_{\text{new}}}\left(\sum_{i=1}^{n}\text{var}_i-\text{var}_{\text{old}}\right)$ 并发送给其他群组成员。

3) UE_i 计算 $g_{k_{\text{new}}}\equiv\text{GK}_{\text{new}}\ (\text{mod}x_i)$ 得到更新后的组密钥。

5.4.2　新成员加入

当附近节点 UE_{new} 加入群组时，服务器执行以下操作更新组密钥 $g_{k_{\text{new}}}$。

1) 服务器选择随机数 $g_{k_{\text{new}}}\in Z_{q/4}^*$ 作为新的组密钥。

2) 计算 $\text{GK}_{\text{new}}=g_{k_{\text{new}}}\left(\sum_{i=1}^{n}\text{var}_i+\text{var}_{\text{new}}\right)$ 并发送

给所有群组成员。

3) UE_i 计算 $g_{k_{new}} \equiv GK_{new} (\mathrm{mod}\ x_i)$ 得到更新后的组密钥。

6 安全评估

6.1 安全分析

1) 双向认证和会话密钥建立。服务器能够使用群组的公共公钥对群组的聚合认证请求进行验证，从而完成对整个群组节点的身份认证。因为公共公钥是由组密钥和群组成员的公钥以非线性方式生成的，所以只有群组内的所有成员一起才能够生成有效的群组聚合请求。群组成员能够使用服务器的公钥对服务器的签名进行验证，从而验证服务器的身份，实现双向认证。群组成员使用私钥只能解密分发给自己的随机数，并不能获得其他分发信息的有关内容，使用解密得到的随机数生成会话密钥，实现了会话密钥的建立并保证了会话密钥的机密性。

2) 重放攻击抗性。在协议认证过程中，使用了时间戳 T_u 和 T_c，并用签名保护了消息的完整性，因此攻击者即使执行重放攻击，也会因为时间戳的时效性失效而攻击失败。

3) 中间人攻击抗性。因为椭圆曲线离散对数难题的求解困难性，认证过程中的随机数 r_i, r_c 的安全性可以得到保证。攻击者并不了解群组成员的私钥，所以也不能够伪造群组认证消息。又因为攻击者不知道群组密钥，所以也不能够伪造服务器的回复消息。中国剩余定理保护了分发随机数的安全性，并建立了群组成员和服务器之间的会话密钥，防止后续通信被窃听和篡改的可能。

4) 认证信令堵塞避免。在所提协议中，大规模 NB-IoT 节点的认证请求会由群组 Leader 收集聚合为群组聚合认证请求，再发送给服务器进行身份认证，大大减少了信令数量并简化了认证流程。同时，使用基于中国剩余定理的方式分发密钥信息，有效减少了服务器回复的数据量和带宽消耗。

5) 内部人攻击抗性。①服务器侧：服务器在注册阶段结束以后，会删除 UE_i 的私钥 x_i，仅保存 var_i 用于后续会话密钥信息的分发。因此，服务器侧的内部攻击者也不能从数据库中盗取到节点的私钥从而伪装成节点进行恶意攻击。②设备群组内部：由于聚合签名和群组公共公钥的生成都使用了非线性的方式，因此群组内的攻击者在不了解其他成员私钥的情况下不能够独自或排除某些成员生成合法的聚合签名。会话密钥信息必须使用对应节点的私钥才能解密得到，而群组内部攻击者在没有得到其他成员私钥的情况下，只使用自身的私钥和群组组密钥，不能够生成其他节点的会话密钥从而伪装成组内其他节点或窃取到其他节点发送的数据。

6.2 协议安全验证工具仿真

本节使用协议形式化分析工具 Scyther[25]对本文所提协议进行安全性仿真分析。Scyther 工具可以对协议进行形式化的描述，仿真验证协议的机密性和可认证性是否存在安全风险，支持无限会话轮数的分析，除了支持 Dolev-Yao 模型和强安全模型外，还支持自定义安全模型，在搜索攻击、安全证明方面非常有用。Scyther 工具采用多种形式的身份验证声明，例如 Nisynch、Niagree、Alive 和 Weakagree 等来检测重放攻击、中间人攻击等安全攻击，使用 SKR 声明来验证协议执行过程中生成密钥的机密性。

本文主要分析以下 3 个角色：群组节点 UE_i、群组 Leader 和服务器，在工具中分别表示为 UE_i、Leader 和 Server。在本文所提协议中，初始化阶段、注册阶段和组密钥更新阶段可以认为是安全的，因此，仅考虑双向认证阶段。采用 Dolev-Yao 攻击者模型对协议进行安全分析。在该模型中，攻击者被认为可以完全控制整个网络中的通信并执行一系列的攻击，包括窃听、拦截、伪造消息等。将本文所提协议在 Scyther 工具中建模，并指定声明协议的安全属性，如图 2 所示。从图 2 中可以看出，经过 Scyther 工具的仿真分析，并未发现可行的安全攻击，说明协议具有可靠的安全性。

Scyther results : verify

Claim				Status	Comments
Protocol	UEi	Protocol,UEi1	Nisynch	Ok	No attacks within bounds.
		Protocol,UEi2	Niagree	Ok	No attacks within bounds.
		Protocol,UEi3	Alive	Ok	No attacks within bounds.
		Protocol,UEi4	Weakagree	Ok	No attacks within bounds.
		Protocol,UEi5	Secret ri	Ok	No attacks within bounds.
		Protocol,UEi6	SKR ki	Ok	No attacks within bounds.
	Leader	Protocol,Leader1	Nisynch	Ok	No attacks within bounds.
		Protocol,Leader2	Niagree	Ok	No attacks within bounds.
		Protocol,Leader3	Alive	Ok	No attacks within bounds.
		Protocol,Leader4	Weakagree	Ok	No attacks within bounds.
	Server	Protocol,Server1	Nisynch	Ok	No attacks within bounds.
		Protocol,Server2	Niagree	Ok	No attacks within bounds.
		Protocol,Server3	Alive	Ok	No attacks within bounds.
		Protocol,Server4	Weakagree	Ok	No attacks within bounds.
		Protocol,Server5	SKR ki	Ok	No attacks within bounds.

Done.

图 2 Scyther 工具的正式安全分析结果

7　性能分析

本节从传输开销、带宽消耗和计算负载等方面分析本文所提协议的性能表现，并同其他现有的群组认证协议进行比较，包括 GAKA[6]、DGBAKA[7]、MTCAKA[8]、SEAKA[9]、EGAKA[10]、GBAAM[12]、GRAKA[13]、LGTH[11]和 FADTS[17]。本节所使用的符号定义如表 2 所示。

表 2　　符号定义

符号	定义
m	节点群组的数量
n	NB-IoT 节点的数量
t_h	执行一次哈希运算的时间
t_m	执行一次点乘运算的时间
t_p	执行一次双线性配对的运算时间

7.1　传输开销

由于传输一次的功耗开销与距离、数据量等多种因素相关，为了便于分析对比本文所提协议和其他现有协议的传输开销，假设 NB-IoT 节点 UE_i 与服务器进行一次传输的开销为一个单位，UE_i 与群组内节点、Leader 进行一次传输的开销为 a 个单位，UE_i 与 NB-IoT 网络的中 eNB 进行一次传输的开销为 b 个单位。由于群组中 UE_i 之间的距离一般不超过 100 m，因此群组间的传输开销远小于一个单位。通常，UE_i 与 eNB 之间的传输开销会因为 UE_i 的部署情况而不同，但是 eNB 与服务器之间的通信因为主要通过有线信道进行传输，因此传输开销可以认为是固定的。根据文献[17]，对传输开销进行简化分析，令 a=0.01，b=0.8。不同协议之间的传输开销对比如表 3 和图 3 所示。从表 3 和图 3 中可以发现，本文所提协议的传输开销与 FADTS 协议相当，远小于其他现有协议。

表 3　　不同协议的传输开销对比

协议	传输开销
GAKA	$(7+2b)n$
DGBAKA	$(7+2b)n$
MTCAKA	$(7+2b)n$
SEAKA	$(7+2b)n$
EGAKA	$(7+2b)n$
GBAAM	$(a+2+2b)n+(a+2)m$
GRAKA	$(a+3+2b)n+4m$
LGTH	$(2a+2+2b)n+4m$
FADTS	$2an+(2a+2)m$
本文所提协议	$2an+(2a+2)m$

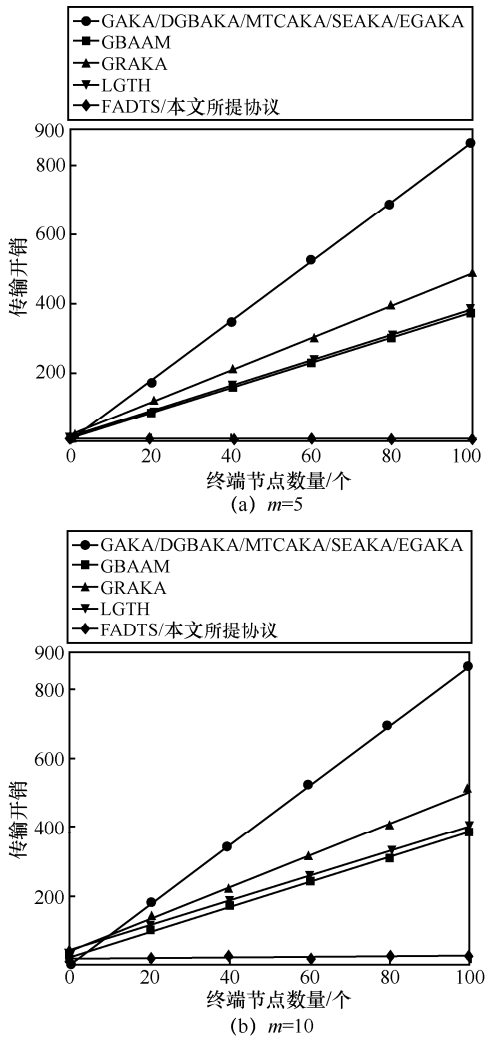


图 3　传输开销对比

7.2　带宽消耗

通过对比传输的数据量大小，来分析对比本文所提协议和其他现有协议的带宽消耗，不失一般性，不同参数的带宽消耗如表 4 所示。

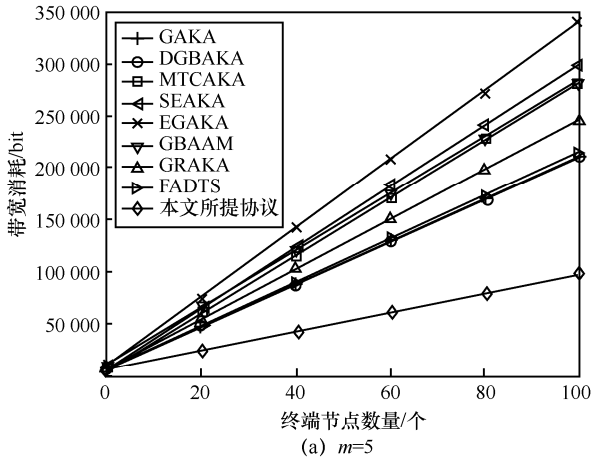
表 4　　不同参数的带宽消耗

参数	带宽消耗/bit
ID/GID/E-RAB(ID)/TEID/LBI	128
Hash	64
随机数	128
PDU	128
GTK/GEK/CK/IK	128
TFT/QOS	80
AMF	48
LAI/POS	40
基于 ECDH 的签名	320
ECHD 密钥	192
时间戳	17

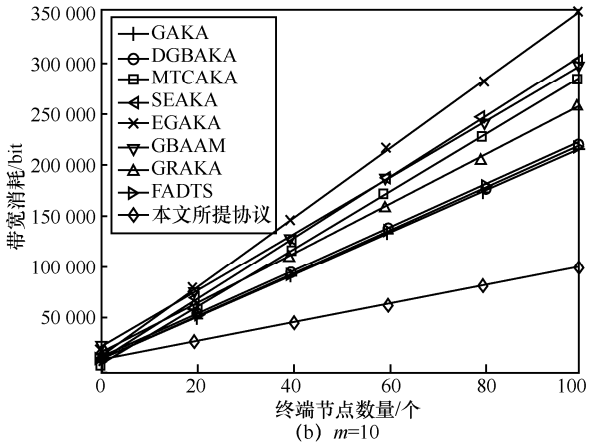
根据所有消息的大小，现有协议的带宽消耗对比如表 5 所示。图 4 显示了在不同分组数量下，不同协议之间总的带宽消耗对比。从图 4 中可以发现，本文所提协议的带宽消耗远小于其他协议。

表 5　　不同协议的带宽消耗对比

协议	带宽消耗/bit
GAKA	2 048n+1 008m
DGBAKA	2 048n+1 264m
MTCAKA	2 784n+432m
SEAKA	2 928n+856m
EGAKA	3 328n+1 344m
GBAAM	2 722n+2 146m
GRAKA	2 385n+1580m
FADTS	2 099n+977m
本文所提协议	894n+1 114m



(a) m=5



(b) m=10

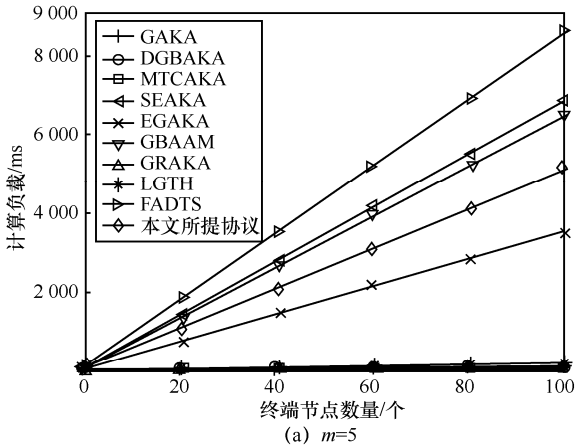
图 4　总带宽消耗对比

7.3　计算负载

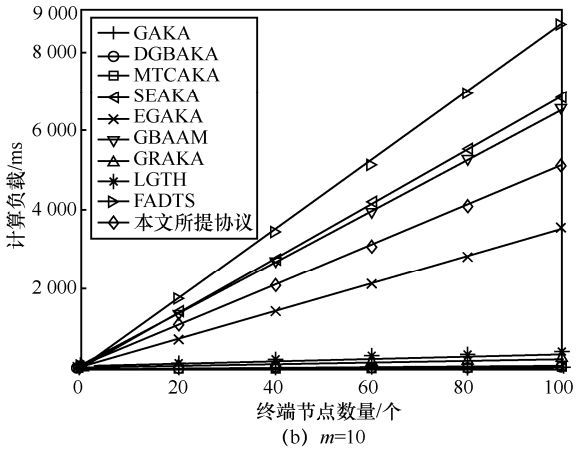
协议认证过程中的计算负载主要考虑以下 3 种加密操作，哈希运算 t_h、点乘运算 t_m 和双线性配对操作 t_p。这 3 种加密操作的计算负载时间如表 6 所示，其中数据使用芯片为 NuvoTon N32905U1DN（ARM926EJ-S@200 MHz）的 ARM9 节点测试得到，服务器数据由配置为 Intel i3-4160@3.60 GHz 的 Dell 个人电脑测试得到。图 5 显示了节点数量和完成认证过程中所需的总计算负载之间的关系。表 7 显示了不同协议计算负载对比。从图 5 中可以发现，本文所提方案计算负载小于 FADTS、SEAKA 和 GRAKA，高于 EGAKA，由于使用了公钥机制来提高安全性，因此远高于其他仅使用哈希函数的方案。

表 6　　加密操作所需时间

加密操作	UE /ms	服务器/ms
t_h	0.049	0.0037
t_m	17.025	0.2834
t_p	659.202	15.4941



(a) m=5



(b) m=10

图 5　计算负载对比

表 7　不同协议计算负载对比

协议	UE /ms	服务器/ms
GAKA	$4t_h$	$3nt_h$
DGBAKA	$9t_h$	$3nt_h$
MTCAKA	$5t_h$	$3nt_h$
SEAKA	$4t_h + 2t_m$	$n(3t_h + 2t_m)$
EGAKA	$7t_h + 2t_m$	$n(2t_h + 2t_m)$
GBAAM	$t_h + 2t_m$	$2n(t_h + t_p)$
GRAKA	$(4m+2)t_h$	$4mt_m$
LGTH	$7mt_h$	mt_h
FADTS	$2t_h + 5t_m$	$(3n+m)t_h + (4n+m)t_m$
本文所提协议	$3t_h + 3t_m$	$(n+2m)t_h + 3mt_m$

8　结束语

针对 NB-IoT 网络中节点大规模接入认证时的通信堵塞问题，本文提出了一种基于 Schnorr 聚合签名和中国剩余定理的新型群组身份安全认证协议。该协议能够一次性对群组中的节点进行身份认证，还有效减少了认证过程中的带宽消耗。协议使用基于 Schnorr 聚合签名的方式生成群组聚合身份认证请求，将聚合请求的大小固定为确定值。协议又采用了基于中国剩余定理的密钥分发方式，使服务器能够以固定大小的回复信息完成对群组中所有节点密钥的分发，将群组与服务器之间的认证通信数据量确定为一固定值，不会随群组中节点的数量而变化，有效减少了认证过程中的带宽消耗。性能分析表明，与其他现有协议相比，所提协议在传输开销和带宽消耗方面性能优异。Scyther 工具对所提协议进行了形式化的安全分析，仿真结果表明，所提协议具有可靠的安全性能。

参考文献：

[1] WANG Y P E, LIN X Q, ADHIKARY A, et al. A primer on 3GPP narrowband Internet of things[J]. IEEE Communications Magazine, 2017, 55(3): 117-123.

[2] ZAYAS A D, MERINO P. The 3GPP NB-IoT system architecture for the Internet of things[C]//Proceedings of 2017 IEEE International Conference on Communications Workshops (ICC Workshops). Piscataway: IEEE Press, 2017: 277-282.

[3] SHI J, JIN L P, LI J, et al. A smart parking system based on NB-IoT and third-party payment platform[C]//Proceedings of 2017 17th International Symposium on Communications and Information Technologies (ISCIT). Piscataway: IEEE Press, 2017: 1-5.

[4] LI Y K, CHENG X, CAO Y, et al. Smart choice for the smart grid: narrowband Internet of things (NB-IoT)[J]. IEEE Internet of Things Journal, 2018, 5(3): 1505-1515.

[5] ZHANG H B, LI J P, WEN B, et al. Connecting intelligent things in smart hospitals using NB-IoT[J]. IEEE Internet of Things Journal, 2018, 5(3): 1550-1560.

[6] CHEN Y W, WANG J T, CHI K H, et al. Group-based authentication and key agreement[J]. Wireless Personal Communications, 2012, 62(4): 965-979.

[7] ZHANG Y Y, CHEN J, LI H, et al. Group-based authentication and key agreement for machine-type communication[J]. International Journal of Grid and Utility Computing, 2014, 5(2): 87.

[8] LAI C Z, LI H, LI X Q, et al. A novel group access authentication and key agreement protocol for machine-type communication[J]. Transactions on Emerging Telecommunications Technologies, 2015, 26(3): 414-431.

[9] LAI C Z, LI H, LU R X, et al. SE-AKA: a secure and efficient group authentication and key agreement protocol for LTE networks[J]. Computer Networks, 2013, 57(17): 3492-3510.

[10] JIANG R, LAI C Z, LUO J, et al. EAP-based group authentication and key agreement protocol for machine-type communications[J]. International Journal of Distributed Sensor Networks, 2013, 9(11): 304601.

[11] LAI C Z, LI H, LU R X, et al. LGTH: a lightweight group authentication protocol for machine-type communication in LTE networks[C]//Proceedings of 2013 IEEE Global Communications Conference (GLOBECOM). Piscataway: IEEE Press, 2013: 832-837.

[12] CAO J, MA M D, LI H. GBAAM: group-based access authentication for MTC in LTE networks[J]. Security and Communication Networks, 2015, 8(17): 3282-3299.

[13] LI J G, WEN M, ZHANG T. Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks[J]. IEEE Internet of Things Journal, 2016, 3(3): 408-417.

[14] LAI C Z, LI H, LU R X, et al. SEGR: a secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks[C]//Proceedings of 2014 IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2014: 1011-1016.

[15] LAI C Z, LU R X, ZHENG D, et al. GLARM: group-based lightweight authentication scheme for resource-constrained machine to machine communications[J]. Computer Networks, 2016, 99: 66-81.

[16] REN X P, CAO J, MA M D, et al. A novel PUF-based group authentication and data transmission scheme for NB-IoT in 3GPP 5G networks[J]. IEEE Internet of Things Journal, 2021, PP(99): 1.

[17] CAO J, YU P, MA M D, et al. Fast authentication and data transfer scheme for massive NB-IoT devices in 3GPP 5G network[J]. IEEE Internet of Things Journal, 2019, 6(2): 1561-1575.

[18] ZHANG Y H, REN F Y, WU A, et al. Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks[J]. IEEE Access, 2019, 7: 114721-114730.

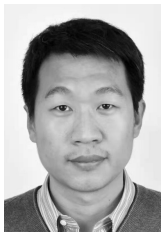
[19] YU P, CAO J, MA M D, et al. Quantum-resistance authentication and data transmission scheme for NB-IoT in 3GPP 5G networks[C]//Proceedings of 2019 IEEE Wireless Communications and Networking Conference (WCNC). Piscataway: IEEE Press, 2019: 1-7.

[20] CAO J, YU P, XIANG X Y, et al. Anti-quantum fast authentication and data transmission scheme for massive devices in 5G NB-IoT system[J]. IEEE Internet of Things Journal, 2019, 6(6): 9794-9805.

[21] MAXWELL G, POELSTRA A, SEURIN Y, et al. Simple Schnorr multi-signatures with applications to Bitcoin[J]. Designs, Codes and Cryptography, 2019, 87(9): 2139-2164.

[22] NI J B, LIN X D, SHEN X S. Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(3): 644-657.
[23] VIJAYAKUMAR P, BOSE S D, KANNAN A. Chinese remainder Theorem based centralised group key management for secure multicast communication[J]. IET Information Security, 2014, 8(3): 179-187.
[24] MAURYA A K, SASTRY V N. User authentication scheme for wireless sensor networks and Internet of things using Chinese remainder theorem[C]//Communications in Computer and Information Science. Singapore: Springer Singapore, 2017: 79-94.
[25] ZHANG J, CUI J, ZHONG H, et al. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(2): 722-735.
[26] KUNG Y H, HSIAO H C. GroupIt: lightweight group key management for dynamic IoT environments[J]. IEEE Internet of Things Journal, 2018, 5(6): 5155-5165.
[27] KOBLITZ N, MENEZES A, VANSTONE S. The state of elliptic curve cryptography[J]. Designs, Codes and Cryptography, 2000, 19(2/3): 173-193.
[28] SCHNORR C P. Efficient identification and signatures for smart cards[C]//Conference on the Theory and Application of Cryptology. Berlin: Springer, 1989: 239-252.
[29] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.
[30] SCHNORR C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3): 161-174.

[作者简介]



常相茂（1982− ），男，山东淄博人，博士，南京航空航天大学副教授，主要研究方向为低功率无线传输技术、智能感知系统等。

占俊（1997− ），男，江西抚州人，南京航空航天大学硕士生，主要研究方向为 NB-IoT 技术。

王志伟（1976− ），男，江苏扬州人，博士，南京邮电大学教授，主要研究方向为可证明安全的密码体制、密码协议、抗量子攻击的公钥密码体制等。