



椭圆曲线加密结合 cookie 信息的物联网终端安全认证协议

赵洁¹, 张华荣²

(1. 江苏第二师范学院数学与信息技术学院, 江苏 南京 210013;

2. 南京师范大学科技处, 江苏 南京 210023)

摘要:针对物联网(IoT)中终端设备接入网络服务器的安全性问题,提出了一种基于椭圆曲线加密(ECC)和 cookie 信息的物联网终端安全认证协议。协议首先将用户身份信息、服务器私钥、随机数和 cookie 有效期信息组成一个 cookie 文件,然后利用椭圆曲线加密体制对其进行加密,并将之存储在智能终端。在认证阶段,通过比对由 cookie 信息计算的安全参数来实现相互身份认证。性能分析表明,该协议在具有较低计算和通信成本的同时,能够有效抵抗多种攻击,提供了较高的安全性,非常适合应用于物联网中资源有限的终端设备。

关键词:物联网;终端设备;身份认证;椭圆曲线加密;cookie 信息

中图分类号:TP309

文献标识码:A

doi: 10.11959/j.issn.1000-0801.2016116

Security authentication protocol based on elliptic curve cryptography and cookie information for terminal of IoT

ZHAO Jie¹, ZHANG Huarong²

1. Department of Mathematics and Information Technology, Jiangsu Second Normal College, Nanjing 210013, China

2. Department of Science and Technology, Nanjing Normal University, Nanjing 210023, China

Abstract: For the security problem of terminal devices accessing to the network server in internet of things (IoT), an identity authentication protocol was presented based on elliptic curve cryptography (ECC) and cookie information for internet of things terminal. Firstly, the protocol used user identity information, server private key, random number and expiration time of cookie to form a cookie file. Then, it was encrypted with ECC and stored in the smart terminal. In authentication phase, the mutual authentication was achieved by comparing the security parameters calculated by cookie information. Performance analysis shows that it can resist many kinds of attacks and provide high security, low computation and low communication cost, which was suitable for the terminal devices of limited resources in internet of things.

Key words: internet of things, terminal device, identity authentication, elliptic curve cryptography, cookie information

收稿日期:2016-01-07;修回日期:2016-03-16

基金项目:国家自然科学基金资助项目(No.61170298);江苏第二师范学院“十二五”规划课题(No.JSNU2014QZ02)

Foundation Items: The National Natural Science Foundation of China(No.61170298), The Foundation of “12th Five-Year” in Jiangsu Second Normal College(No.JSNU2014QZ02)

1 引言

物联网(internet of things, IoT)是在计算机互联网基础上,将各种信息传感设备(如嵌入式设备、RFID等)与互联网结合,形成的一个巨大的实物互联网络^[1]。随着物联网的迅速发展,大量嵌入式设备连接到互联网进行信息交换和数据通信,这对安全性提出了很高的要求。由于物联网的很多嵌入式终端设备资源有限,传统安全协议无法在其上直接应用,而针对嵌入式设备的各种攻击越来越多,如假冒、窃听、重放、拒绝服务攻击等^[2],因此安全问题已经成为物联网发展中的关键问题之一。

目前,针对物联网的安全传输问题,业界已开展了深入研究,主要集中在终端与服务器之间的认证研究,通常采用的方法有基于散列函数的认证、基于状态的认证、基于密钥加密的认证等^[3]。在基于密钥加密的方法中,椭圆曲线加密(elliptic curve cryptography, ECC)^[4]机制利用较小尺寸的密钥提供了较高的安全性,且适用于资源有限的嵌入式设备,因此出现了多种基于ECC的身份认证协议。例如,参考文献[5]提出了一种用于保证智能设备和服务器之间安全性的ECC认证协议,并证明了ECC比其他公钥加密(public key cryptography, PKC)技术更有效性。参考文献[6]提出了一种基于ECC的智能卡远程认证方案,但因其没有密钥协商阶段,故导致其易受到重复攻击。参考文献[7]基于ECC提出了一种基于轻属性加权的加密协议,一定程度上解决了多项式认证机制存在的计算复杂问题,降低了认证消耗,但安全性不够高,不能抵抗字典攻击,且不具备匿名性保护。参考文献[8]提出了一种用于物联网中RFID系统的ECC身份认证协议,利用ECC生成公钥和私钥,并通过生成的随机数动态计算验证信息来实现标签认证,可有效抵抗安全攻击,但存在被跟踪的隐私安全问题。参考文献[9]提出了一种基于ECC的身份认证传输协议,但计算复杂度较高,且不能抵御中间人和字典攻击。

目前,物联网中的终端智能设备大都配备Web浏览器,使其能够接入网络。在访问网络时,终端设备会产生一个cookie文件^[10],记录用户的访问信息。本文受其启发,在终端设备访问网络时,也构建了一个cookie文件,并将其与ECC进行结合,构建了一种低计算复杂度、高安全性的身份认证协议,用于物联网终端设备和云服务器之间的安全通信。其中,本文认证方案所适用的物联网终端设备为具有一定计算能力和支持HTTP访问物联网服务器功能

的智能终端,例如智能传感设备、手机等移动手持设备。与现有基于ECC的认证协议相比,本文所提协议在保持较低计算成本的同时,提供了较高的安全性能,非常适合用于物联网系统中嵌入式终端设备的安全认证。

2 椭圆曲线加密机制

在提供相同级别安全性的基础上,相比于其他非对称加密技术,椭圆曲线加密(ECC)具有更小的密钥尺寸^[11]。例如,一个256 bit的对称密钥必须由大于15 000 bit的RSA来保护,然而,仅用512 bit的ECC非对称密钥就可以提供相等的安全性,因而可有效节约计算成本。

通常,加密系统的安全性与基本数学问题的相对复杂性成正比。若将一个算法的时间复杂度表达为多项式 $T(n)=o(n^k)$ 且取上界,则该算法是一个多项式时间算法,其中, n 为输入的尺寸, k 为非负整数。ECC的安全性取决于解决椭圆曲线离散对数问题(elliptic curve discrete logarithm problem, ECDLP)^[12]的难度。

在ECDLP中, P 和 Q 为椭圆曲线上的两个点, kP 代表添加到其本身 k 倍的点,其中 k 是一个标量, $kP=Q$ 。对已知的 P 和 Q ,若 k 足够大,则不可能计算出 k 。 k 为 Q 到基 P 的离散对数。

ECC的数学运算在椭圆曲线方程上的定义为 $y^2=x^3+ax+b$,其中, $4a^3+27b^2\neq 0$ 。

椭圆曲线是满足上述方程的解 (x,y) 的集合。 a 和 b 的每个值给出了一个不同的椭圆曲线。满足上述方程和无穷远处点 O 的所有点 (x,y) 均位于椭圆曲线上。

在ECC点乘运算中,椭圆曲线上的 P 利用椭圆曲线方程乘以一个标量 k ,即获得椭圆曲线上的另一点 Q ,如 $kP=Q$ 。通过两种基本的椭圆曲线操作,即点加运算和倍点运算来实现点乘运算。

3 提出的认证协议

在物联网中,为连接网络,嵌入式设备通常配置一个Web浏览器和TCP/IP协议栈,使其作为HTTP客户端^[13]。cookie是由Web服务器生成并存储于用户计算机内存中的文本信息,是实现Web应用认证的主要手段,由cookie名称、有效期、目录和站点域等信息组成。对嵌入式HTTP设备,在安全认证中融入cookie信息有助于提高其安全性。

为此,本文提出了一种基于ECC和cookie信息的安全认证协议,用于物联网系统中的嵌入式设备。其中,ECC



主要用于密钥加密,使之对应椭圆曲线上的密文点,利用椭圆曲线离散对数问题来实现密钥的安全传输和签名认证。表1为本文所提协议用到的符号及其含义。

表1 本文协议用到的符号及含义

符号	含义
D_i	嵌入式设备
S	云服务器
ID_i	设备 D_i 的身份
P_i	设备 D_i 的密码
R_i	服务器生成的随机数
N_1, N_2	ECC 参数生成的随机数
$H()$	单向散列函数
X	基于 ECC 的服务器的私钥
Z_p	有限域组
p	阶 $>2^{160}$ 的大素数
G	大阶数 n 的生成点
CK	cookie 信息
EXP_TIME	cookie 的有效时间
$ $	级联运算
$\oplus$	异或运算

本文所提协议包括3个阶段:注册阶段,嵌入式设备在云服务器上进行注册,服务器将 cookie 存储在嵌入式设备上;登录阶段,当设备需要与服务器连接时,在这一阶段发送登录请求;认证阶段,嵌入式设备和云服务器利用 ECC 参数进行相互认证。图1描述了本文所提协议的工作流程。

在系统开始运行前,服务器 S 在 Z_p 上选择一个椭圆曲线方程 $y^2=x^3+ax+b$,其中 $Z_p(p>2^{160})$ 为有限域组。服务器选择两个域元素 $a, b \in Z_p$,其中, a 和 b 满足条件 $4a^3+27b^2 \pmod p \neq 0$ 。令 G 为含有 $n(n>2^{160})$ 个素数阶的椭圆曲线的基本点, O 为无穷点,则 $n \times G = O$ 。服务器选择一个随机数 X 作为它的私钥。

3.1 注册阶段

首先,嵌入式设备 D_i 在云服务器 S 上进行注册,发送唯一的 ID_i 到服务器;云服务器收到这个请求后,为每个设备 D_i 生成一个唯一的密码 P_i 。

步骤1 $D_i \rightarrow S: ID_i$, 服务器 S 生成 P_i 。

服务器为每个设备选择一个唯一的随机数,并生成一个 cookie $CK = H(R_i | X | EXP_TIME | ID_i)$, 其中, X 为服务器的私钥。同时,服务器将该 cookie 存储在嵌入式设备上,作为 ECC 点 $CK' = CK \times G$ 。然后,服务器计算安全性参数 $T_i = R_i \oplus$

服务器EP: $y^2=(x^3+ax+b) \pmod p$ 超过 Z_p
其中 $(4a^3+27b^2) \pmod p \neq 0, p>2^{160}$
 X : 服务器的私钥; $PS=(X \times G)$: 服务器的公钥
 G : 生成点; $X \times G = O, n>2^{160}$

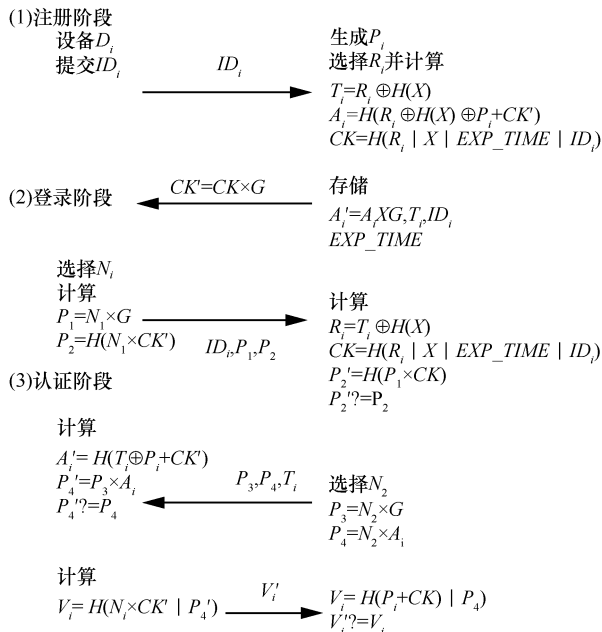


图1 本文所提协议的工作流程

$H(X), A_i' = H(R_i \oplus H(X) \oplus P_i + CK')$, 并将 $A_i' = H(R_i \oplus H(X) \oplus P_i + CK') \times G$ 和对应设备 D_i 身份 ID_i 的 T_i 存储在数据库中。服务器自己存储对应该 cookie 的有效时间 EXP_TIME 。当 cookie 过期时,将有效时间更新为 EXP_TIME' ,并将 cookie 更新为 $CK = H(R_i | X | EXP_TIME' | ID_i)$ 。

步骤2 $S \rightarrow D_i$: cookie CK' 。

3.2 登录阶段

在每次登录前,设备选择一个随机数 N_i ,计算 ECC 点 $P_i = N_i \times G$,并将其存储在它的内存中。

步骤1 D_i 计算 ECC 点 P_i 。

为登录云服务器,设备计算 ECC 点 $P_2 = H(N_i \times CK')$,并发送 P_1, P_2 和它的 ID_i 到服务器。

步骤2 $S \rightarrow D_i$: cookie CK' 。

3.3 认证阶段

服务器在收到登录请求的参数后,首先使用其私钥 X 计算来自 T_i 的随机数 $R_i = T_i \oplus H(X)$;然后,利用其私钥、设备身份 ID_i 和有效时间 EXP_TIME 计算 cookie 信息 $CK = H(R_i | X | EXP_TIME | ID_i)$;接着计算点 $P_2' = H(P_i \times CK)$,并核对

P_2' 的值是否等于接收到的 P_2' 值,若相等,则服务器执行下一个步骤,否则服务器终止会话。

步骤 1 S 核对 $P_2' = P_2; S \rightarrow D_i: P_3, P_4$ 和 T_i 。

服务器选择一个随机数 N_2 , 计算 ECC 点 $P_3 = N_2 \times G, P_4 = N_2 \times A_i'$, 并发送 P_3, P_4 和 T_i 到嵌入式设备。

步骤 2 嵌入式设备核对 $P_4' = P_4; D_i \rightarrow S: V_i$ 。

设备收到信息后, 计算 $A_i = H(T_i \oplus P_i \oplus CK')$ 和 ECC 点 $P_4' = P_3 \times A_i$, 并将 P_4' 的值与接收到的 P_4 值进行比较。若相等, 则嵌入式设备计算 $V_i = H((N_1 \times CK') | P_4')$ 并发送 V_i 到服务器。

步骤 3 服务器核对 $V_i' = V_i$ 。

服务器计算 $V_i' = H((P_1 \times CK') | P_4)$, 并将该值与收到的 V_i 进行比较以认证该设备。

在嵌入式设备和云服务器相互认证后, 两者共同协商一个会话密钥 $SK = H(X | ID_i | N_1 | N_2)$, 用于后续在设备与云服务器之间进行的通信。

4 安全性分析

(1) 抵抗重放攻击

重放攻击是指在认证过程中, 攻击者窃听服务器和设备之间的通信信息, 并重发这些消息, 以试图达成通过系统认证、充当合法用户进行登录的目的^[4]。

在本文所提协议中, 利用唯一新值 N_1 生成椭圆曲线点 P_1 , 利用单向散列函数生成 P_2 。当恶意设备试图利用新值 N' 登录时, 在服务器认证信息时会失败。若攻击者试图利用先前的 P_1 和 P_2 值计算点 $P_1'' = N' \times P_1$ 和 $P_2'' = N' \times P_2$, 则在第一步认证阶段会失败。这是因为服务器利用新值计算的点 $P_2'' = N' \times H(P_1' \times CK)$ 与期望值 $P_2' = H(N' \times G \times CK)$ 不相等。因此, 本文所提协议可以抵抗重放攻击。此外, 恶意用户不能重发登录信息, 这是因为它不能访问 N_1 或 CK' 的值, 这使得它不能生成 $V_i = H((P_1 \times CK') | P_4')$ 。还有, 它不能重复使用相同的 P_4 值进行重放, 这是因为 P_4 取决于 N_3 , 而 N_3 是服务器为每次认证随机生成的新值。

(2) 抵抗中间人攻击

中间人攻击类似于重放攻击, 攻击者通过冒充合法服务器发送从设备中获得的响应消息来模仿合法设备。

在中间人攻击中, 恶意用户可能会收集通信参数, 如 CK', P_1, P_2, P_3 和 P_4 。在本文所提协议中, 由于这些点有很高的熵, 因此恶意用户无法计算这些 ECC 点, 在真正的多项式时间内解决 ECDLP 是不可能的。此外, 恶意用户不知

道随机新值 N_1 和 N_2 。因此, 本文所提协议能够抵抗中间人攻击。

(3) 抵抗 cookie 盗窃攻击

在 cookie 盗窃攻击中, 攻击者从智能设备中窃取存储在其中的 cookie 信息, 并试图利用该信息登录云服务器 S 。但在本文所提协议中, cookie 信息 $CK = H(R_i | X | EXP_TIME | ID_i) \times G$ 被存储为一个 ECC 点, 因此不能利用该信息来获得登录所需的正确参数。此外, 在任何消息通信中, 本文所提协议不发送 cookie CK 到服务器, 这样, 即使恶意用户可能得到 cookie CK , 该信息也几乎毫无用处。因此, 本文所提协议能够抵抗 cookie 盗窃攻击。

(4) 抵抗窃听攻击

由于服务器和嵌入式设备之间的通信消息通过不安全通道传输, 因此攻击者可以通过窃听获取用户的机密信息, 并利用窃听信息伪造合法用户的身份来认证信息^[5]。

在本文所提协议中, 当攻击者试图修改从 ID_i, P_1 和 P_2 进入 ID_i^*, P_1^* 和 P_2^* 的登录请求时, 恶意用户无法获取随机数 N_1 和 N_2 。此外, P_1 和 P_2 的熵非常高, 故 ECC 不能被伪造。因此这类攻击将在认证阶段的第一步遭遇失败。

(5) 抵抗暴力破解攻击

在暴力破解攻击中, 恶意用户首先从通信消息中获得参数 P_1, P_2, P_3, P_4 和 T_i 。在本文所提协议中, 即使恶意用户成功记录这些信息, 仍无法利用暴力破解攻击找出正确的密码 P_i , 这是因为他不知道服务器的密钥 X 且没有办法猜测随机数 N_1 和 N_2 。因此, 本文所提协议可以抵抗暴力破解攻击。

(6) 抵抗离线字典攻击

在这种类型的攻击中, 恶意用户首先记录通信消息, 接着尝试从这些信息中猜测合法用户的密码。在本文协议中, 恶意用户不能在多项式时间内从作为高熵 ECC 点的记录通信消息中计算出密码。因此, 本文所提协议可以抵抗离线字典攻击。

(7) 抵抗认证器泄漏攻击

在这种类型的攻击中, 恶意用户进入服务器并窃取存储在其中的信息, 然后利用这些信息计算合法用户的密码。在本文所提协议中, 存储在设备数据库中的信息为 $CK = H(R_i | X | EXP_TIME' | ID_i), A_i' = H(R_i \oplus H(X) \oplus P_i) \times G$, 这是一个 ECC 点, 故恶意用户不能猜测服务器的私钥 X 或 ECC 点 A_i' 。因此, 本文所提协议可以抵抗认证器泄漏攻击。



(8) 提供相互身份认证

在本文所提协议中,服务器通过比较收到的 P_2 值和计算 P_2' 值来检查智能设备的真实性。设备利用方程 $P_2 = H(N_1 \times CK')$ 计算 P_2 值,其中, $CK' = CK \times G$, 并将其发送给服务器。接着,服务器利用方程 $P_2' = H(P_1 \times CK)$ 计算值 P_2' , 其中, $P_1 = N_1 \times G$ 。若值相等,则该服务器成功认证此用户。另外,用户通过比较收到的 P_4 值和计算的 P_4' 值来认证服务器。服务器利用方程 $P_4 = N_2 \times A_i'$ 计算 P_4 值并将其发送给设备,其中 $A_i' = A_i \times G$ 。接着,设备利用方程 $P_4' = P_3 \times A_i$ 计算 P_4' 值,其中, $P_3 = N_2 \times G$ 。若这两个值相等,则设备成功认证服务器。

(9) 提供机密性保护

本文所提协议利用 ECC 点和散列函数来保护设备认证信息,确保只有经过认证的设备才能访问服务器。因此,本文所提协议可以抵抗流量分析和窃取,保证信息机密性。

(10) 提供匿名性保护

通常设备可以发送用于认证的消息到其附近的任何服务器。如果攻击者冒充服务器来接触设备,则该设备将与攻击者交换初始消息。本文协议中,攻击者不能访问与设备有关的 $cookie(CK')$,不能生成 $A_i' = H(T_i \oplus P_i \oplus CK') \times G$ 的正确值,从而不能生成正确的 $P_4 = N_2 \times A_i'$ 值。接收到的 P_4 值与期望值 $P_4' = P_3 \times A_i$ 进行认证会失败,其中, $A_i = H(T_i \oplus P_i \oplus CK')$ 。因此,本文所提协议可以提高匿名性。

(11) 提供前向保密性

前向保密性指的是利用设备当前的传播信息不能追踪先前的传播信息。由于在每次会话中,随机产生的新值提供了机密性,即恶意用户没法知道设备内生成的随机数,因此本文通过使过去的通信信息具有不可预测性来确保前向保密性。

5 成本分析

一个有效的身份认证协议必须考虑计算和通信成本。本文使用了 XOR 操作和单向散列函数,这些在密码学中都是计算量较低的操作。在本文协议中,设置身份 ID_i 、密码 P_i 、新值 (N_1, N_2) 、随机数 R_i 和安全性参数 T_i, R_i 都为 128 bit;同时,单向散列函数的输出也为 128 bit,椭圆曲线公钥密码 ECC 为 224 bit。

令 T_H 表示一次散列运算, T_E 表示一次指数运算, T_{ECM} 表示一次椭圆曲线上的点乘运算, T_{ECA} 表示一次椭圆曲线上的点加运算,这些运算的时间复杂性比较结果为: $T_E \geq T_{ECM} > T_{ECA} > T_H$, 其中,执行一次指数运算消耗的时间比执行

一次椭圆点乘运算大很多(约 8 倍)^[20]。此外,在本文协议中没有使用时间戳,因此不存在时间同步问题。

(1) 通信成本

协议的通信成本 C1 是指安全参数的传输成本。在本文所提协议中,传输的安全参数为 $[P_1, P_2, P_3, P_4, T_i, ID_i] = [4 \times 224 + 3 \times 128] = 1280$ bit。

(2) 计算成本

令 C2 为注册阶段中由服务器执行的所有操作消耗的总时间,在本文所提协议中为 $(3T_H + 2T_{ECM})$;令 C3 为认证阶段中云服务器的计算成本,为 $(4T_H + 4T_{ECM})$;令 C4 为认证阶段中嵌入式设备用于计算的时间,为 $(3T_H + 3T_{ECM})$ 。

(3) 存储成本

令 C5 为嵌入式设备所需内存, C6 为服务器用于存储安全参数所需内存,在本文所提协议中,嵌入式设备将 $cookie CK'$ 储存为 ECC 点,因此 $C5 = 224$ bit。云服务器储存 (A_i', ID_i) , 因此 $C6 = 224 + 128 = 352$ bit。

6 性能比较

将现有基于 ECC 的认证协议与本文所提协议在安全与成本方面进行比较。表 2 对各种协议提供的功能和攻击抵抗能力进行了比较,其中,“是”表示具有该功能或能够抵抗该攻击,“否”表示不具备该功能或不能抵抗该攻击,“-”表示不涉及该项目。可以看出,与现有协议相比,本文所提协议能够提供全面的功能且能够抵御常见类型的攻击。

表 3 给出了各种协议的计算、通信和存储成本,可以看出,本文所提协议具有较低的成本,这就使其非常适合用于资源有限的物联网嵌入式终端设备中。

7 结束语

由于现有安全认证协议不能直接用于保护物联网中嵌入式设备和云服务器之间的安全通信,为此,本文提出了一种基于 ECC 和 $cookie$ 信息的高效安全认证协议。性能分析表明,本文所提协议有效降低了计算、通信和存储成本,使其适合用于资源有限的智能终端设备上。此外,本文所提协议提供了双向认证、机密性、匿名性和前向安全性,能够抵抗常见的多种身份攻击模式,具有很高的安全性能。在今后的研究工作中,将考虑采用轻量级 ECC 来进一步提高其认证速度,以期最终形成一种快速、高效的安全协议。

表 2 安全性能比较

功能	参考文献[5]	参考文献[6]	参考文献[7]	参考文献[8]	参考文献[9]	本文协议
双向认证	否	是	是	是	是	是
密钥协商	否	否	是	否	是	是
无需时钟同步	是	是	否	是	是	是
匿名性	是	是	否	否	是	是
前向安全性	是	是	是	是	是	是
重放攻击	否	否	是	是	是	是
中间人攻击	是	是	是	否	否	是
cookie 盗窃攻击	-	-	-	-	-	是
窃听攻击	是	否	是	是	是	是
离线字典攻击	否	是	否	是	否	是

表 3 成本性能比较

成本	参考文献[5]	参考文献[6]	参考文献[7]	参考文献[8]	参考文献[9]	本文协议
计算成本 (服务器)	$4T_H + 8T_{ECM} + 2T_{ECA}$	$3T_H + 6T_{ECM} + 2T_{ECA}$	$7T_H + 14T_{ECM}$	$1T_E + 4T_{ECM} + 2T_{ECA}$	$8T_{ECM} + 5T_{ECA}$	$7T_H + 6T_{ECM}$
计算成本 (设备)	$5T_{ECM} + 2T_{ECA}$	$3T_{ECM} + 2T_{ECA}$	$3T_H + 2T_E + 8T_{ECM}$	$1T_E + 3T_{ECM} + 3T_{ECA}$	$4T_{ECM} + 2T_{ECA}$	$3T_H + 3T_{ECM}$
通信成本/bit	1 280	1 216	1 280	1 280	1 680	1 280
内存成本/bit	352	224	448	256	652	224

参考文献：

[1] 吴振强, 周彦伟, 马建峰. 物联网安全传输模型[J]. 计算机学报, 2011, 34(8): 1351-1364.
WU Z Q, ZHOU Y W, MA J F. A security transmission model for internet of things[J]. Chinese Journal of Computers, 2011, 34(8): 1351-1364.

[2] 汪礼臻, 张龙军. 适合物联网环境的混合双向匿名认证协议[J]. 计算机应用研究, 2015, 32(1): 222-225.
WANG L Z, ZHANG L J. Hybrid mutual anonymous authentication protocol for the internet of things environment[J]. Application Research of Computers, 2015, 32(1): 222-225.

[3] 唐雅玲. 一种基于认证的物联网安全传输机制 [J]. 计算机工程, 2014, 40(1): 144-148.
TANG Y L. A secure transmission mechanism for internet of things based on certification[J]. Computer Engineering, 2014, 40(1): 144-148.

[4] 黄碧翼, 陈泽茂, 朱婷婷. 基于椭圆曲线签密协议的无线安全认证协议[J]. 武汉理工大学学报, 2013, 35(6): 145-150.
HUANG B Y, CHEN Z M, ZHU T T. Wireless security authentication protocol based on elliptic curve signcrypton scheme [J]. Journal of Wuhan University of Technology, 2013, 35(6): 145-150.

[5] ZHAO G, SI X, WANG J, et al. A novel mutual authentication scheme for internet of things[C]// IEEE International Conference on Modelling, Identification and Control (ICMIC), June 26-29, 2011, Shanghai, China. New Jersey: IEEE Press, 2011: 563-566.

[6] LI C T. A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card[J]. Iet Information Security, 2013, 7(1): 3-10.

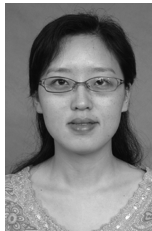
[7] SHEN G, ZHEN Y. Application of elliptic curve cryptography in node authentication of internet of things [C]// 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, October 16-18, 2013, Beijing, China. New Jersey: IEEE Press, 2013: 452-455.

[8] SHIVRAJ V L, RAJAN M A, SINGH M, et al. One time password authentication scheme based on elliptic curves for internet of things (IoT) [C]// 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), February 17-19, 2015, Riyadh, Kingdom of Saudi Arabia. New Jersey: IEEE Press, 2015: 1-6.



- [9] HE D, ZEADALLY S. An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography[J]. Internet of Things Journal IEEE, 2015, 2(1): 72-83.
- [10] 冯伟华, 刘亚丽. 基于 cookie 的统一认证系统的设计与实现[J]. 计算机工程与设计, 2010, 31(23): 4971-4975.
- FENG W H, LIU Y L. Design and implementation of unified authentication system on cookie[J]. Computer Engineering and Design, 2010, 31(23): 4971-4975.
- [11] 张文芳, 王小敏, 郭伟, 等. 基于椭圆曲线加密体制的高效虚拟企业跨域认证协议[J]. 电子学报, 2014(6): 1095-1102.
- ZHANG W F, WANG X M, GUO W, et al. An efficient inter-enterprise authentication scheme for VE based on the elliptic curve cryptosystem[J]. Acta Electronica Sinica, 2014(6): 1095-1102.
- [12] 刘柱文, 李丽琳. 新的基于椭圆曲线的三方口令认证密钥协商协议[J]. 计算机应用, 2011, 31(10): 2687-2688.
- LIU Z W, LI L L. New three-party password-based authenticated key agreement protocol with elliptic curve[J]. Journal of Computer Applications, 2011, 31(10): 2687-2688.
- [13] BENINI L. Designing next-generation smart sensor hubs for the internet-of-things [C]// 5th IEEE International Workshop on Advances in Sensors and Interfaces (IWASI), June 13-14, 2013, Bari, Italy. New Jersey: IEEE Press, 2013: 113.
- [14] CHEN P Y, CHENG S M, CHEN K C. Information fusion to defend intentional attack in internet of things [J]. Internet of Things Journal IEEE, 2014, 1(4): 337-348.
- [15] 冯福伟, 李瑛, 徐冠宁, 等. 基于集群架构的物联网身份认证系统[J]. 计算机应用, 2013, 33(1): 126-129.
- FENG F W, LI Y, XU G N, et al. IoT authentication system based on cluster architecture[J]. Journal of Computer Applications, 2013, 33(1): 126-129.

[作者简介]



赵洁(1979-),女,江苏第二师范学院数学与信息技术学院讲师,主要研究方向为信息安全及物联网。



张华荣(1980-),女,南京师范大学科技处助理研究员,主要研究方向为管理科学与工程。