基于国密 SM9 的工业边缘计算场景身份认证方案

陈 卓[1,2] 蒋秋璐[1,2] 王明月[1,2]
CHEN Zhuo JIANG Qiulu WANG Mingyue

摘 要 边缘服务器和智能设备是工业边缘计算场景中的核心设备，其安全可信的运行是确保整个工业系统稳定、可靠、防止重大生产事故和商业机密泄露的基石。身份认证作为保障工业边缘计算场景安全可信的第一道防线，可以有效防止恶意的攻击者冒充合法设备。传统的基于公钥证书的认证方案由于其复杂繁琐的证书传输和管理会给工业边缘计算的网络和设备带来难以承受的开销，而基于身份标识密码的国密 SM9 算法正好弥补了此缺陷，无需申请和交换证书。因此，文章提出了一种基于国密 SM9 的工业边缘计算场景身份认证方案，该认证方案能够实现边缘服务器对智能设备的接入验证，并且具有机密性、前向安全性、抵御篡改攻击、抵御重放攻击和抵御假冒攻击等安全特性。此外，实验仿真与分析表明，文章提出的身份认证方案在保证安全性的同时，耗时较少、效率较高。

关键词 工业物联网；边缘计算；国密 SM9；身份认证

doi：10.3969/j.issn.1672-9528.2026.02.016

0 引言

工业物联网（industrial internet of things, IIoT）作为物联网技术在工业领域的核心应用[1]，将推进工业体系数字化和智能化的变革。然而，随着网络边缘侧的设备数量及其产生的数据量爆发式增长，传统的云计算模式[2]在实时性、带宽成本以及数据安全与隐私等方面出现不足。因此，边缘计算[3]应运而生，其与工业物联网深度融合将构建一个层次分明、反应快速、安全可靠的工业边缘智能化系统。在工业边缘计算场景中，核心设备主要有两类：一类设备是边缘服务器，负责处理和分析来自智能设备的海量数据，运行机器学习模型进行智能决策，具有较强的计算和存储能力；一类设备是智能设备，如智能机器人、智能机械臂和智能摄像机等，负责采集工业现场的数据并执行控制指令。显然，工业边缘计算场景的安全和可信运行就特别重要。身份认证作为保障工业边缘计算场景安全的第一道防线[4-5]，可以构建各个设备之间的初始信任基石，可以防止恶意攻击者冒充合法设备获取访问权限及系统资源。任何未经授权的设备接入或非法指令的注入，都可能导致生产中断、次品率攀升，甚至引发灾难性的安全事故。

基于公钥证书的认证方案（如标准的 TLS/SSL）[6]，虽然安全性高，但其冗重的证书链传输以及繁琐的证书生命周期管理，会给工业边缘计算的设备和网络带宽带来难以承受的开销。相比之下，基于身份标识密码（identity-based cryptograph, IBC）的身份认证方案[7]，不涉及复杂的证书传输和管理，适合于工业边缘计算场景。国密 SM9 算法[8]即 IBC 的典型代表，该算法可以用设备的身份信息作为标识，进行相应的身份认证，无需申请和交换证书，速度快、能耗小，能够在工业边缘计算场景中灵活部署。

本文基于国密 SM9 算法，面向工业边缘计算场景提出了一个身份认证方案，该身份认证方案能够实现边缘服务器对智能设备的接入验证，只有签名合法，通过验证的智能设备才能访问或者上传数据到边缘服务器，保护工业边缘计算场景中的重要敏感数据。此外，本文的身份认证方案还具有机密性、前向安全性、抵御篡改攻击、抵御重放攻击和抵御假冒攻击等安全特性。

1 系统模型

1.1 系统架构

本文所提出的基于国密 SM9 的工业边缘计算场景身份认证方案的系统架构如图 1 所示，该认证方案有三类参与方，分别是边缘服务器、智能设备和密钥管理服务器。其中边缘服务器具有较强的计算和存储能力，能够对智能设备上传的数据进行智能化处理，并进行智能决策。智能设备，如智能

1. 重庆移通学院 重庆 401420
2. 公共大数据安全技术重庆市重点实验室 重庆 401420

[基金项目] 重庆市綦江区科技计划项目“基于区块链与零信任协同的分布式网络安全体系构建与关键技术研究”（2025032）；重庆移通学院应用研究项目“区块链赋能的零信任动态安全体系研究”（KY202510）

机器人、智能机械臂和智能摄像机等，是工业现场的数据采集终端和执行终端。密钥管理服务器是一个具有高安全性和可信度的实体，能够在工业边缘计算环境中生成系统所需要的安全参数，并发送给相应的实体。

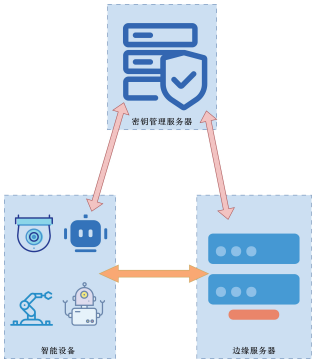

图 1 系统架构图

1.2 安全目标

安全目标主要是针对公共信道中的恶意攻击者，该攻击者可以拦截公共信道上的消息，并且还可以篡改公共信道上的消息。本文的身份认证方案所实现的安全目标如下：

（1）机密性：机密性指的是智能设备和边缘服务器之间的秘密信息必须得到保护，攻击者无法在公共信道上获取到这些秘密信息。

（2）前向安全性：前向安全性指的是如果某次认证会话的签名被破解，之前的签名不受影响，之前的签名和认证会话是安全的。

（3）抵御篡改攻击：篡改攻击指的是攻击者可以捕获公共信道上的认证会话消息，并且篡改它。

（4）抵御重放攻击：重放攻击指的是攻击者可以捕获前一个认证会话的消息，并在当前会话中重放它，以达到欺骗边缘服务器的目的。

（5）抵御假冒攻击：假冒攻击指的是攻击者可以假冒合法的智能设备，以达到欺骗边缘服务器的目的，可以访问边缘服务器里面的重要敏感数据。

2 认证方案设计

2.1 系统初始化阶段

（1）输入安全参数 λ，密钥管理服务器生成素数阶为 N 的加法循环群 G_1、G_2，以及乘法循环群 G_T，循环群 G_1、G_2 的生成元分别为 P_1、P_2。

（2）密钥管理服务器选择一个随机数 $s \in [1, N-1]$ 作为系统主私钥，并计算相应的系统公钥 P_{pub}：

$$P_{pub}=sP_2 \tag{1}$$

选取双线性对 $e:G_1\times G_2\rightarrow G_T$，然后选择两个安全的哈希函数（国密 SM3 算法 [9]）$H_1:\{0,1\}^* \rightarrow Z_N^*$，$H_2:\{0,1\}^* \rightarrow Z_N^*$。

（3）密钥管理服务器发布公共参数 $\{G_1, G_2, N, P_1, P_2, P_{pub}, H_1, H_2\}$ 给系统内的所有设备。

2.2 设备注册阶段

在设备注册阶段，智能设备通过安全信道与密钥管理服务器交互生成其完整的公钥和私钥。

智能设备将自己身份标识 ID_s 发送给密钥管理服务器，密钥管理服务器在有限域 F_N 上计算 t_s 与 u_s：

$$t_s = H_1(ID_s,N)+s \tag{2}$$

$$u_s = s\cdot t_s^{-1} \tag{3}$$

然后计算其私钥 d_s，计算公式为：

$$d_s = u_sP_1 = \frac{s}{H_1(ID_s,N)+s}P_1 \tag{4}$$

以及其公钥 Q_s，计算公式为：

$$Q_s = H_1(ID_s, N)P_1+P_{pub} \tag{5}$$

计算完成以后，密钥管理服务器将 $\{d_s, Q_s\}$ 发送给智能设备。

2.3 认证阶段

在认证阶段，智能设备向边缘服务器发送认证请求，边缘服务器根据认证请求决定智能设备是否接入，具体流程如图 2 所示。

（1）智能设备计算 g：

$$g=e(P_1, P_{pub}) \tag{6}$$

选择一个随机数 $r_s \in [1, N-1]$，计算 ω_s：

$$\omega_s=g^{r_s} \tag{7}$$

以及计算 h_s，计算公式为：

$$h_s=H_2(T_1 // \omega_s, N) \tag{8}$$

式中：T_1 为时间戳。

（2）智能设备计算 L_s，计算公式为：

$$L_s=(r_s-h_s) \bmod N \tag{9}$$

然后计算 σ_s，计算公式为：

$$\sigma_s=L_sd_s \tag{10}$$

然后把签名 $\{h_s, \sigma_s\}$ 和时间戳 T_1 发送给边缘服务器。

（3）边缘服务器收到智能设备发送的签名 $\{h_s, \sigma_s\}$ 和时间戳 T_1 以后，首先生成一个时间戳 T_2，验证 $|T_2-T_1| \le \Delta T$，其中 ΔT 为边缘服务器与智能设备之间约定的延迟时间，如果不在此时间内，边缘服务器则立即终止通信，拒绝此认证请求。如果在延迟时间内，边缘服务器验证 $h_s \in [1, N-1]$ 与 $\sigma_s \in G_1$ 是否成立，若不成立则终止通信。

（4）边缘服务器计算 g：

$$g=e(P_1,P_{pub}) \tag{11}$$

计算 t、$h_s^{'}$ 和 P，计算公式为：

$$t=g^{h_s} \tag{12}$$

$$h_s^{'}=H_1(\mathrm{ID}_s,N) \tag{13}$$

$$P=h_s^{'}P_2+\mathrm{P_{pub}} \tag{14}$$

（5）边缘服务器计算 μ、$\omega_s^{'}$ 和 $h_s^{''}$，计算公式为：

$$\mu=e(\sigma_s,P) \tag{15}$$

$$\omega_s^{'}=\mu\cdot t \tag{16}$$

$$h_s^{''}=H_2(T_1 /\!/ \omega_s^{'},N) \tag{17}$$

然后检验 $h_s^{''}=h_s$ 是否成立，如果成立，则验证通过，边缘服务器同意智能设备的接入；如果不成立，则拒绝接入，并立即终止通信。

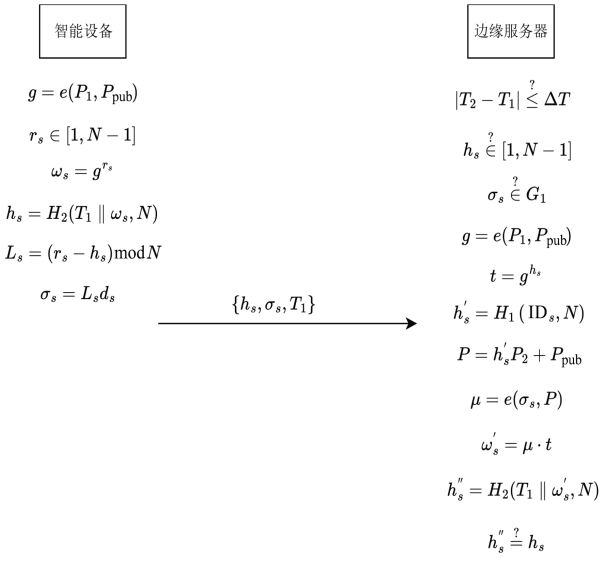

图 2 认证阶段流程图

3 正确性和安全性分析

3.1 正确性分析

本文的身份认证方案满足计算正确性，即只有合法的智能设备才能产生正确的签名并通过边缘服务器的验证。根据双线性配对的性质，验证 $h_s^{''}=h_s$ 是否相等，需要先验证 $\omega_s^{'}$ 与 ω_s 是否相等：

$$\begin{aligned}\omega_s^{'}&=\mu\cdot t=e(\sigma_s,P)\cdot t=e\left(L_sd_s,h_s^{'}P_2+P_{\mathrm{pub}}\right)\cdot t\\&=e\left(L_sd_s,\left(h_s^{'}+s\right)P_2\right)\cdot t=e(d_s,P_2)^{L_s\left(h_s^{'}+s\right)}\cdot t\\&=e\left(\frac{s}{h_s^{'}+s}P_1,P_2\right)^{L_s(h_s^{'}+s)}\cdot t=e(P_1,P_2)^{\mathrm{SL}_s}\cdot t\\&=g^{L_s}\cdot t=g^{L_s}\cdot g^{h_s}=g^{r_s-h_s+h_s}=g^{r_s}\\&=\omega_s\end{aligned} \tag{18}$$

然后，由于 $\omega_s^{''}=\omega_s$，所以：

$$h_s^{''}=H_2\left(T_1 /\!/ \omega_s^{'},N\right)=H_2(T_1 /\!/ \omega_s,N)=h_s \tag{19}$$

因此，等式 $h_s^{''}=h_s$ 成立。通过正确性证明，可以得出本文的身份认证方案满足正确性。

3.2 安全性分析

本文提出的身份认证方案具有机密性、前向安全性、抵御篡改攻击、抵御重放攻击和抵御假冒攻击等安全特性。

（1）机密性

密钥管理服务器的系统主私钥 s，主要是由密钥管理服务器秘密保存，即使攻击者获取到系统公钥 P_{pub}，也由于椭圆曲线离散对数难题（ECDLP）[10] 获取不了系统主私钥 s。智能设备的私钥 d_s 是密钥管理服务器通过安全信道秘密发送的，所以攻击者获取不了。综上所述，系统主私钥 s 与智能设备的私钥 d_s 攻击者获取不了，本文的身份认证方案实现了机密性。

（2）前向安全性

智能设备生成的签名与随机数 r_s 有关，因为每次认证生成的随机数 r_s 都不一样，所以每次认证生成的签名 $\{h_s, \sigma_s\}$ 也都不一样。即使一次认证会话的签名被破解，也不会危及之前的签名，即之前的签名和认证会话是安全可信的。因此，本文的身份认证方案实现了前向安全性。

（3）抵御篡改攻击

如果在认证会话中，攻击者篡改了认证会话消息，那么这种恶意行为会被边缘服务器检测到。如攻击者篡改了签名 $\{h_s, \sigma_s\}$，首先边缘服务器会验证 h_s 是否在 [1, N−1] 范围内，以及 σ_s 是否是群 G_1 上的有效点，只要有其一不满足，则边缘服务器会拒绝此签名，如果都满足，然后边缘服务器会验证 $h_s^{''}=h_s$ 是否成立，由于哈希函数的抗碰撞性 [11]，只要有 h_s 或 σ_s 被恶意篡改，都会导致 $h_s^{''}=h_s$ 不成立。若攻击者篡改了时间戳 T_1，同样，由于哈希函数的抗碰撞性，时间戳 T_1 篡改会导致 $h_s^{''}=h_s$ 不成立。综上所述，本文的身份认证方案能够抵御篡改攻击。

（4）抵御重放攻击

本文的认证方案是通过时间戳机制 [12] 来抵御重放攻击的，来自之前会话的认证消息的传输延迟将会超过约定的延迟时间 ΔT。如果攻击者修改了时间戳 T_1，由于哈希函数的抗碰撞性，这会导致 $h_s^{''}=h_s$ 不成立。因此，本文的身份认证方案能够抵御重方攻击。

（5）抵御假冒攻击

如果有攻击者想要假冒智能设备接入到边缘服务器当中，访问边缘服务器的敏感重要数据，这是不可行的。只有拥有合法智能设备的私钥 d_s，才能产生合法的签名，而私钥 d_s 是由密钥管理服务器生成，并通过安全信道发给智能设备，攻击者是伪造不了的，并且也获取不了的。因此，本文的身份认证方案能够抵御假冒攻击。

4 实验仿真与分析

本实验是在 VMware Workstation 虚拟机上仿真运行的，该虚拟机运行的是 Ubuntu 22.04.5 LTS 操作系统，内存 4 GB，处理器 Intel Core i7-14700F。采用 C 语言，基于 Miracl 密码库 [13]，实现了本认证方案的认证阶段，即签名与验证过程。

签名结果如图 3 所示，其中 h 为签名 $h_s=H_2(T_1 // \omega_s, N)$ 的哈希值，σ_{s_x} 与 σ_{s_y} 为签名 σ_s 的 x 与 y 坐标。签名一次的时间为 2.626 ms。

```
begin test
签名成功!
h:  ==================
\x04\x00\x00\x00\x00\x00\x00\x00\x58\x31\xf8\x0d\xd2\x58\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\xb0\x36\x05\xc2\x73\xc5\xbf\x9c
σs_x: ==================
\x04\x00\x00\x00\x00\x00\x00\x00\xf8\xb2\xf8\x0d\xd2\x58\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x9c\xdd\xe7\x46\x15\x95\x00\x94
σs_y: ==================
\x04\x00\x00\x00\x00\x00\x00\x00\x28\xb7\xf8\x0d\xd2\x58\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\xa8\xcf\xe3\x8a\x58\xc9\x2e\x51
签名 1 次，总时间: 2.626 毫秒
```

图 3 签名结果

验证结果如图 4 所示，其中 h_2 为 $h_s''=H_2(T_1 // \omega_s', N)$ 的哈希值，可以看出此哈希值与图 3 签名结果图的 h 即 $h_s=H_2(T_1 // \omega_s, N)$ 的哈希值一样，所以验证通过。验证一次的时间为 8.164 ms。

```
h2:  ==================
\x04\x00\x00\x00\x00\x00\x00\x00\x38\xe2\xfa\x0d\xd2\x58\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\xb0\x36\x05\xc2\x73\xc5\xbf\x9c
验证 1 次，总时间: 8.164 毫秒
```

图 4 验证结果

结合签名和验证时间，总的时间为 10.79 ms。由此可见，本文的认证方案在保证安全性的同时，耗时较少，效率较高。

5 结语

本文提出了一种基于国密 SM9 的工业边缘计算场景身份认证方案，该认证方案无需复杂繁琐的证书传输和管理，能够实现边缘服务器对智能设备的接入验证，防止恶意的攻击者冒充合法智能设备，保护工业边缘计算场景的安全。同时，该身份认证方案具有机密性、前向安全性、抵御篡改攻击、抵御重放攻击和抵御假冒攻击等安全特性。实验仿真与分析表明，该认证方案签名和验证耗时较少，适合于工业边缘计算场景。

参考文献：

[1] 张学旺，陈思宇，罗欣悦，等 . 面向云辅助工业物联网的高效可搜索属性基加密方案 [J]. 信息网络安全，2024, 24(9): 1352-1363.

[2] 王爽，李小平，陈龙 . 云环境下随机请求性能分析综述 [J]. 计算机学报，2022,45(6):1241-1260.

[3] 李森森，黄一才，黄美根，等 . 面向移动边缘计算的高效条件隐私保护认证密钥协商方案 [J]. 通信学报，2025, 46(9): 195-212.

[4] 李哲成，张波 . 基于区块链的轻量级工业物联网跨域认证与数据共享方案 [J]. 计算机研究与发展，2025, 62(10): 2416-2427.

[5] 吴毅，冯涛，柳春岩，等 . 基于工业物联网的分层多设备认证密钥协商协议 [J]. 网络与信息安全学报，2025,11(4):86-106.

[6] 林璟锵，荆继武，张琼露，等 .PKI 技术的近年研究综述 [J]. 密码学报，2015, 2(6): 487-496.

[7] 黄仁季，吴晓平，李洪成 . 基于身份标识加密的身份认证方案 [J]. 网络与信息安全学报，2016, 2(6):32-37.

[8] 谢振杰，罗友强，赵方方，等 . 基于国密算法 SM9 的签密方案 [J]. 计算机科学，2025,52(S2):818-825.

[9] 田昊，王超 . 基于国密 SM3 和 SM4 算法的 SNMPv3 安全机制设计与实现 [J]. 计算机科学，2024,51(S1):931-937.

[10] 曾丽，李旭东 . 基于椭圆曲线的强无证书盲签名方案 [J]. 网络空间安全，2018,9(5):41-44.

[11] 杨小东，安发英，杨平，等 . 云环境下基于代理重签名的跨域身份认证方案 [J]. 计算机学报，2019,42(4):756-771.

[12] 石庆霞，汪学明 . 新的移动支付协议及其形式化分析 [J]. 计算机应用与软件，2025,42(11):318-324.

[13] 周林，矫文成，吴杨 . 卫星网络密钥管理仿真平台的设计及性能测试 [J]. 计算机技术与发展，2012,22(9):217-220.

【作者简介】

陈卓（1997—），男，重庆人，硕士，助教，研究方向：工业物联网信息安全、身份认证。

蒋秋璐（1997—），女，重庆人，硕士，讲师，研究方向：区块链安全、隐私保护。

王明月（1990—），女，重庆人，博士，副教授，研究方向：大数据安全、物理层安全。

（收稿日期：2025-12-22　修回日期：2026-02-04）