计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2024,33(7):84−93 [doi: 10.15888/j.cnki.csa.009560]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于 CFL 的去中心工控系统签名认证方案①

谢云飞[1], 赵东东[2], 石乐义[1]

[1](中国石油大学 (华东) 计算机科学与技术学院, 青岛 266580)
[2](歌尔科技有限公司, 青岛 266104)
通信作者: 石乐义, E-mail: shileyi@upc.edu.cn

摘　要: 近来, 工业控制系统的身份认证和数字签名等安全问题受到越来越多的关注. 本文将去中心化的 CFL 认证体制引入到工控系统身份认证中, 提出了基于 CFL 的工控系统签名认证方案, 建立了基于 CFL 认证体制的工控系统认证模型 CFL-SYS, 引入 UKey 作为证书载体, 实现了签名验证过程去中心化; 通过计算用户 ID 的哈希值生成随机私钥和标志私钥实现一人一密, 满足了用户对私钥的私有权并且保护了用户的隐私. 理论分析和实验结果表明, 本文方案在吞吐量、系统验证响应时间等性能上能够满足毫秒级应用需求, 能为大规模工业控制系统提供一种自主、可靠、高效的签名认证方案.

关键词: 工业控制系统; 数字身份认证; CFL 认证体制; 去中心化

引用格式: 谢云飞,赵东东,石乐义.基于 CFL 的去中心工控系统签名认证方案.计算机系统应用,2024,33(7):84–93. http://www.c-s-a.org.cn/1003-3254/9560.html

Signature Authentication Scheme for Decentralized Industrial Control System Based on CFL

XIE Yun-Fei[1], ZHAO Dong-Dong[2], SHI Le-Yi[1]

[1](College of Computer Science and Technology, China University of Petroleum, Qingdao 266580, China)
[2](Goertek Inc., Qingdao 266104, China)

Abstract: Recently, security issues such as identity authentication and digital signatures in industrial control systems have received more and more attention. This study introduces the decentralized certificateless (CFL) cryptography authentication system into the identity authentication of the industrial control system and proposes a signature authentication scheme for the industrial control system based on CFL. It builds the CFL-SYS authentication model for the industrial control system based on the CFL authentication system and introduces UKey as the certificated carrier to decentralize the signature verification process. A random private key and a flagging private key are generated by calculating the hash value of the user ID to realize one-person-one-key encryption, which satisfies the user's private ownership of the private keys and protects the user's privacy. Theoretical analysis and experimental results show that the proposed scheme can meet the millisecond-level application requirements in terms of throughput and system verification response time, and can provide an autonomous, reliable, and efficient signature authentication scheme for large-scale industrial control systems.

Key words: industrial control system; digital identity authentication; CFL certification system; decentralization

工业控制系统在电网、石油、交通和智能制造等领域得到广泛应用, 已成为国家关键基础设施的重要组成部分. 随着数字经济的发展, 工控领域的安全问题, 如身份认证和数字签名等, 越来越受到关注, 数据安

① 基金项目: 国家自然科学基金 (61772551); 山东省自然科学基金 (ZR2019MF034)
收稿时间: 2024-01-09; 修改时间: 2024-02-07, 2024-02-27; 采用时间: 2024-03-04; csa 在线出版时间: 2024-06-05
CNKI 网络首发时间: 2024-06-07

全、工控安全和云安全成为热点话题.

根据国家工业信息安全发展研究中心 2020 年的公告, 全球发生的因网络攻击导致的严重安全事件高达 70 多起, 涉及范围广泛, 包括 8 个主要领域和 16 个细分领域. 这说明工业控制系统在面对互联网攻击时的脆弱性. 例如, 2010 年, 伊朗政府宣布核工厂受到“震网”病毒破坏; 2018 年, 加拿大的取水调度系统遭到黑客攻击, 导致取水调度计算机损坏; 2022 年 4 月, 国家工信安全中心发布的《2021–2022 年我国网络安全产融合作发展报告》指出, 我国网络安全产业热度持续上升, 出现了 128 起安全事件, 披露金额达 147 亿. 这些事件显示了工控安全事件日益严重, 迫切需要安全措施来保护工控系统.

目前, 工控系统中普遍采用口令技术进行操作人员身份认证, 但这种方式安全性有限, 容易受到字典攻击. 另外, 许多工厂采用基于生物特征的认证方式, 如人脸识别和指纹识别, 但这种方式需要昂贵的专业验证设备, 且生物特征容易被仿冒. 此外, 我国大部分工控设备和系统依赖进口, 导致一些存在漏洞的国外工控产品在国内仍在使用, 存在严重的安全隐患. 因此, 工控系统急需一种自主、可靠、高效的身份认证方案.

为了解决身份认证的安全问题, 国内外学者进行了一系列的研究, 但是在实际场景中, 认证系统的中心化以及私钥的私有权问题一直是系统安全的瓶颈[1], 且目前在工控领域的身份认证安全问题不受重视, 相关方案也比较少.

美国国家标准与技术研究院 (NIST) 在 2000 年给出了利用公钥技术实现数字签名和认证的指导意见[2], 促进了公钥技术在认证方面的应用. Camenisch 等[3]针对身份的匿名认证, 提出了基于双线性对的签名方案. Boneh 等[4]基于前期提出 BLS 短群签名方案, 可以实现多次的动态认证, 提高了认证的效率. 王中华等[5]通过无证书公钥密码体制, 实现“口令+秘钥”的双因子认证方案, 但是此方案需要保证认证节点服务器在线, 增加了系统的负担.

Hardjono 等[6]在传统 PKI 基础上结合零知识证明提出匿名身份认证模型, 有效解决了身份管理机制问题. Ye 等[7]针对工业控制系统网络中数字证书管理和 PKI 正确部署面临的挑战, 提出 PKI 部署到工控系统的建议方案. 魏珊珊等[8]在以 PLC 为中心的工控系统中给出证书认证模型及 PKI 部署设计, 并采用引擎机制给出国密算法 SM2、SM3 扩展到 OpenSSL 中的关键结构, 提出基于 PKI 的工控系统身份鉴别方式, 但存在证书中心权利过度集中, 使得整体效率和安全性不高.

MacKenzie 等[9]提出 DSA 两方签名的方案, 使得两方签名参与者对公钥生成签名, 任何一方都不能单独实现签名. Lindell 等[10]提出基于 Paillier 同态加密算法的 ECDSA 方案, 该方案直接利用 Paillier 算法的同态属性完成双方的签名, 提高了系统在注册阶段的效率. Doerner 等[11]提出基于秘密共享和不经意传输技术的 (2, n)-门限 ECDSA 方案, 不需要 Paillier 同态加密操作但是引入了不经意传输协议, 使通信开销大大增加. Castagnos 等[12]使用哈希证明技术提出了一种新的 ECDSA 方案, 但整体运行效率却不高. 王婧等[13]针对签名私钥易泄露和签名权利过度集中的问题, 通过预计算一次一密的 Beaver 三元组, 保证 2 个签名参与方在不重构完整签名私钥的情况下输出合法 ECDSA 签名, 但是方案依赖于两方的通信, 整体性能受通信效率的影响.

He 等[14]提出针对 IEEE P1363 标准的两方协同签名方案. 侯红霞等[15]提出两方协作的 SM2 签名算法, 该算法将签名私钥拆成两个部分, 分别由两方来保管, 实现了合法的通信双方协作产生 SM2 签名. Zhang 等[16]提出了 SM2 签名算法的两方分布式签名协议, 也是将私钥分开存储在两个设备上, 达到了防止秘钥泄露的目的, 但是认证双方之间的频繁通信使得系统的响应时间也明显增加, 系统吞吐量受通信速度的影响较严重.

SM2 数字签名算法是国家密码管理局基于椭圆曲线密码体制提出的[17], 能够满足多种密码应用中的身份认证和数据完整性的安全需求, 与 RSA 和 DSA 签名算法相比, SM2 算法依赖于求解椭圆曲线上离散对数问题的困难性[18], 具有更高的安全性和计算效率, 目前已在国内商业密码领域应用多年.

现有的认证体制主要有公开密钥基础设施 (PKI) 证书认证和椭圆曲线数字签名算法 (ECDSA), 但适合工业控制场景的认证体制方案并不多, 随着社会的发展, 这些认证体制已经暴露出严重不足. PKI 认证体制需要可信第三方 (如认证中心 CA) 对证书申请、签发、验证、废止、更新等环节巨大计算资源支持, 难以满足高速度、低消耗的需求. 多方协同的 ECDSA 签名方案虽然解决了签名权利过度集中的问题, 但是依

赖于过多的通信开销, 使得整体效率不高.

密码基础逻辑 (cryptography fundamental logics, CFL) 是由国内学者在 2009 年提出的一种基于标识的证书认证体制[19], 王海平等[20]通过论述得出 CFL 可以解决的问题领域和场景, 其适用于云计算、大数据、工控系统、免疫计算平台等场景. 刘文婷等[21]给出了 CFL 的密钥管理方案, 对 CFL 认证体制进行了进一步完善, 舒展翔等[22]给出了 CFL 在区块链中的具体应用方案, 并通过实验表明系统的正确性和安全性. 王琳等[23]将 CFL 认证体制应用在空间卫星认证领域, 在保证安全性的前提下, 将通信效率提升了 33%. 但是目前将 CFL 认证体制应用于工控设备与工控系统与工作人员认证的具体认证方案还没有被提出, 本文基于此进行研究. 相比较于现有的中心化函数认证体制, CFL 认证体制的实体身份认证过程无须第三方参与, 具有验证过程去中心化的优势, 因此本文提出了 CFL 工控系统签名方案来解决上述问题, 实现工控设备之间与工控设备和工作人员之间的高效认证, 主要贡献可以分为以下 3 个方面.

(1) 设计了一种安全高效的 CFL 工控系统签名方案, 通过计算 ID 的哈希值生成签名私钥和验证公钥实现验证去中心化和一人一密, 同时能够保护用户的隐私.

(2) 提出了设计目标, 并对本文方案进行了安全性分析, 使得本文方案更适合应用于工控系统大规模身份认证的场景.

(3) 从理论分析和实验验证两个方面对本文所提方案进行对比分析, 结果表明, 本文方案在提高身份认证系统整体效率方面具有明显优势.

1 工控系统签名认证方案

1.1 工控系统认证架构

系统应用场景为工控设备启动时和员工对设备进行设置时, 认证系统对操作人员进行一次身份验证, 验证通过后在设备正常工作期间不需验证. 工控系统认证结构如图 1 所示. 下面分别对部署结构中的各组成部分进行简要介绍.

CGC (certificate generation center): 云端的证书生成和注销中心服务器, 负责接收来自注册端的请求并对证书签名, 完成证书的生成和注销.

注册端: 用户使用证书注册设备输入自己的 ID 和创建证书请求, 把 CGC 生成的证书存入 UKey 内[24].

验证端: 对现场工控设备配备具有 USB 接口的验证设备, 在设备启动时对操作人员身份合法性进行一次验证, 当且仅当身份验证通过后, 才允许用户对工控设备进行启动和设置.

工控设备: 工业控制系统的现场工作设备, 用户身份信息认证通过后, 接收用户的指令并按照程序进行相应的动作.

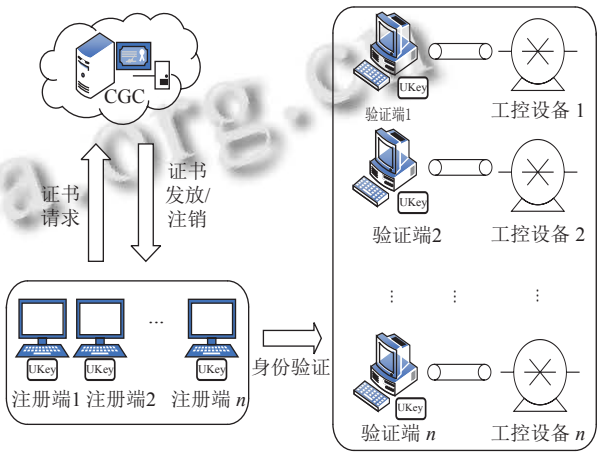

图 1 工控系统认证架构图

1.2 认证方案设计

1.2.1 设计目标

本文提出的 CFL 工控系统签名方案应满足以下 3 个属性.

① 验证过程去中心化. CFL 证书的注册需要通过 CFL-CGC 进行签名, 但 CFL 证书的验证可以在工控系统的其他验证设备上自主进行, 从而减轻了 CFL-CGC 中心的负担.

② 一人一密. 本方案在 CFL-CGC 进行注册时, 根据注册用户 ID 的哈希值不同, 用不同的标志私钥 IDSK 对证书进行签名, 相较于证书生成中心所有签名只用一对公、私钥进行签名的方式, 本文方案更加安全.

③ 用户在 CFL-CGC 进行注册前, 首先使用随机私钥 RASK 进行签名, 然后与 CFL-CGC 的签名进行组合. 此外, 随机私钥 RASK 由用户在本地端自主生成, 一定程度上保护了用户的隐私[25], 进一步提高了 CFL 数字签名方案的隐私性和安全性.

1.2.2 CFL-SYS 工控系统结构图

CFL-SYS 认证体制由 CFL-CGC (CFL-certificate generation center), 注册端和验证端组成, CFL 工控系统认证模型如图 2 所示. 系统共有两个阶段组成, 领卡注

册阶段和插卡验证阶段. 领卡注册阶段由用户插入 UKey 输入自己的工号 ID, 使用注册端的随机私钥 RASK 完成签名并创建证书请求发送到云端 CFL-CGC 服务器, 云端 CFL-CGC 首先审查用户提交的 ID 正确性, 然后通过标识私钥 IDSK 签名得到 CFL 证书, 再将证书返还到注册端并存入 UKey 内, 用户则可以拿着 UKey 到验证设备上进行身份认证[26]. 员工对工业控制系统现场的生产设备进行启动时和设置时, 将 UKey 插入验证设备, 按照算法对证书进行各项验证, 并将最终的结果显示出来, 当且仅当全部验证通过后, 现场设备才会允许员工进行下一步的操作. 同时选用了 SM2 算法[14]作为 CFL 数字签名算法的核心签名算法.

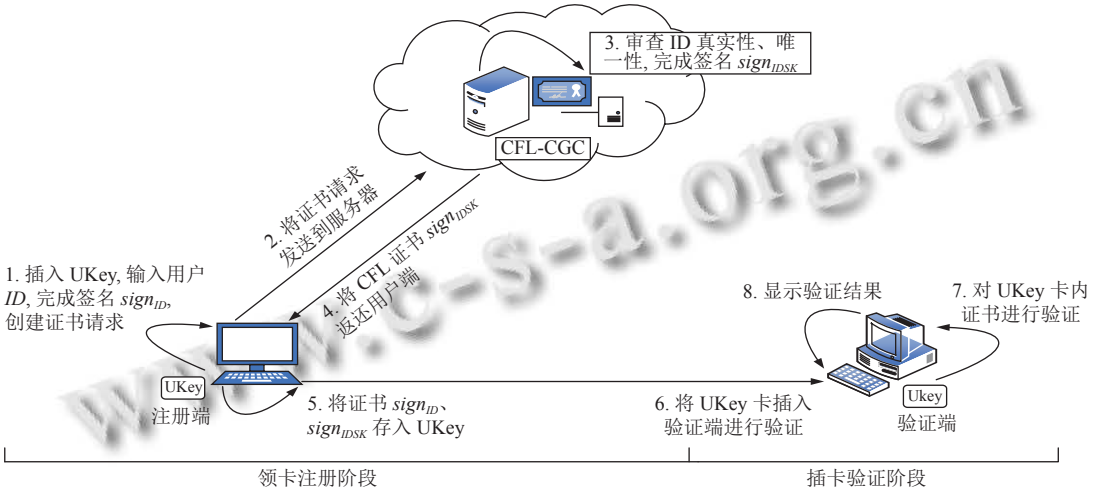

图 2 CFL-SYS 工控系统认证模型

1.2.3 注册流程

注册阶段是用户需要对生产设备进行操作之前, 首先到注册端向 CFL-CGC 创建证书请求, 并将得到的 CFL 证书存入 UKey 内, 完成证书的注册, 如图 3 所示. 其中 CFL-CGC 会根据用户 *ID* 的哈希值选择签名数据库中的标志私钥 *IDSK* 对请求完成签名.

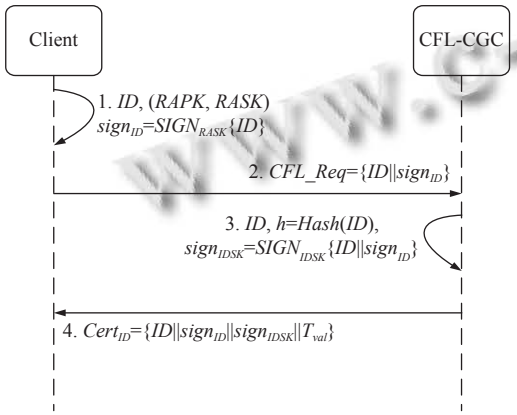

图 3 CFL 注册流程时序图

步骤 1. 用户首先输入自己的工号 *ID*, 然后注册系统会根据用户 *ID* 的哈希值 *h*=*Hash*(*ID*) 生成一组随机公私钥, 用随机私钥 *RASK* 对用户 *ID* 进行签名得 $sign_{ID} = SIGN_{RASK}\{ID\}$, 待用户记下随机私钥后, 注册系统将此随机私钥进行删除.

步骤 2. 用户创建证书申请 $CFL\_Req = \{ID \| sign_{ID}\}$, 将其发送到 CFL-CGC.

步骤 3. CFL-CGC 接收 *CFL_Req* 并对比证书申请内容中的 *ID* 与用户 *ID* 数据库, 确保其满足真实性和唯一性, 验证通过后将 *ID* 输入 *Hash* 函数得 *h*=*Hash*(*ID*), 根据 *h* 生成一组标志公私钥, 用标志私钥 *IDSK* 对证书请求进行签名得 $sign_{IDSK} = SIGN_{IDSK}\{ID \| sign_{ID}\}$, 得到经过 CFL-CGC 签名得 CFL 证书.

步骤 4. CFL-CGC 将 CFL 证书加入有效时间 T_{val}, 打包组成 CFL 证书 $Cert_{ID} = \{ID \| sign_{ID} \| sign_{IDSK} \| T_{val}\}$, 将其发送回用户注册端, 由注册端将 CFL 证书存入 UKey 内.

1.2.4 验证流程

验证阶段是用户得到经过注册的 UKey 后, 到工业控制系统的生产设备上进行操作的身份认证阶段, 如图 4 所示.

步骤 1. 验证端读取 CFL 证书, 会陆续判断证书 *ID*, 有效时间, CFL-CGC 的签名和用户签名的真实性.

步骤 2.1. 验证端首先验证 CFL 证书内员工 *ID* 的真实性和唯一性, 只有员工 *ID* 正常的前提下才能继续验证.

步骤 2.2. 验证端查找 CFL 证书内是否包含注销标识“REVOKE”, 只有证书未被注销的前提下才能继续验证.

步骤 2.3. 计算当前的时间戳$T_{sta} \leqslant Cert_{ID}.T_{val}$, 判断时间戳在 CFL 证书的有效范围之内, 有效时间满足条件后再进行下一步验证.

步骤 2.4. 验证端提取$Cert_{ID}.ID$, 计算 $h=Hash(ID)$, 根据 h 生成标志私钥 *IDSK* 对应的标志公钥 *IDPK*, 验证 CFL-CGC 的签名$sign_{IDSK}$.

步骤 2.5. 根据 h 生成随机私钥对应的随机公钥 *RAPK*, 验证用户的签名$sign_{ID}$.

步骤 3. 验证端向用户界面返回本次的验证结果“TRUE/FALSE”, 告知用户本次验证的结果, 整个身份认证全部通过后, 现场设备才允许用户对设备进行设置和操作.

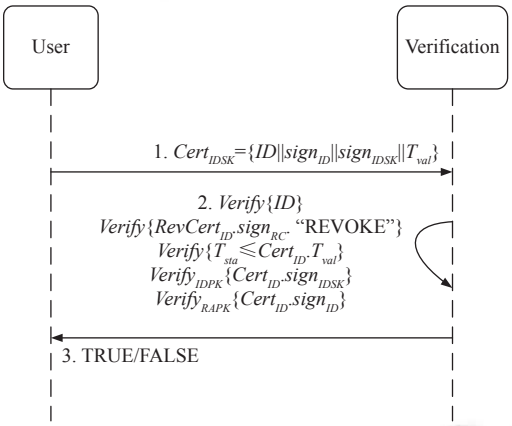

图 4 CFL 验证流程时序图

1.2.5 注销流程

注销阶段是向 CFL-CGC 申请撤销 UKey 内的合法 CFL 证书. 注销后的 CFL 证书将不再具有身份认证的作用, 如图 5 所示.

步骤 1. 用户将 UKey 插入 CFL-CGC 证书生成中心, 以 *RASK* 为密钥, 对$Cert_{ID}$和注销标识“REVOKE”进行签名得$sign_{\mathrm{REV}}$.

步骤 2. 用户向 CFL-CGC 发送证书注销申请 RevReq.

步骤 3. CFL-CGC 用随机公钥 *RAPK* 验证注销签名值$sign_{\mathrm{REV}}$的正确性, 同理按照“插卡验证阶段”的 Step 2.3–Step 2.4 验证$sign_{IDSK}$和$sign_{ID}$.

步骤 4. CFL-CGC 以 *IDSK* 为私钥, 对 *ID* 和注销标识“REVOKE”进行签名得$sign_{\mathrm{RC}}$, 将注销证书$RevCert_{ID}$发送回用户端.

步骤 5. 用户端将 UKey 内的 CFL 证书$Cert_{ID}$更新为$RevCert_{ID}$, 完成整个 CFL 证书注销的过程.

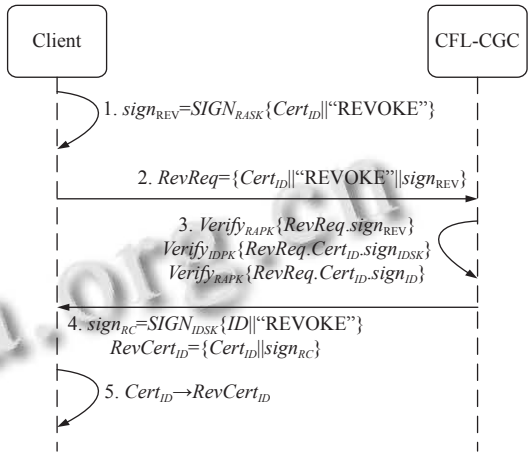

图 5 CFL 注销流程时序图

2 方案分析

BAN 逻辑为协议的形式化分析提供了一种有效的工具[27]. BAN 逻辑只在抽象层次上讨论认证协议的安全性, 并不考虑由协议的具体实现所带来的安全缺陷和由于加密体制的缺点引发的协议缺陷. 本节对 CFL 工控系统签名认证方案进行形式化描述, 并对其安全性进行形式化的分析, 即证明在本方案下用户与 CFL-CGC 证书生成中心和验证设备之间是可互信的.

2.1 用户与 CFL-CGC 中心的认证属性形式化分析

假设用户 *A* 首先向 CFL-CGC 证书生成中心发出证书申请, 然后 CFL-CGC 将经过签名的证书返回用户 *A*, 并存入 UKey 内, 完成 CFL 证书的注册阶段.

步骤 1. 设领卡注册的用户为 *A*, CFL-CGC 中心为 *C*. 协议形式化:

$$A \rightarrow C : \{ID, sign_{ID}\} \tag{1}$$

$$C \rightarrow A : \{ID, sign_{ID}, sign_{IDSK}, T_{val}\} \tag{2}$$

步骤 2. 设$I_0 = \{ID, sign_{ID}\}, I_1 = \{sign_{IDSK}, T_{val}\}$. 初始假设:

$$A \mid\equiv A \overset{I_0}{\rightleftarrows} C \tag{3}$$

$$A \triangleleft \{I_0, I_1\} \tag{4}$$

$$A \mid\equiv \#(I_1) \tag{5}$$

$$A \mid\equiv C \Rightarrow I_1 \tag{6}$$

步骤 3. 协议目标:

$$A \mid\equiv I_1$$

步骤 4. 推理验证:

由初始假设式 (3) 和式 (4) 以及公钥消息含义推理可得:

$$\frac{A \mid\equiv C \overset{I_0}{\rightleftarrows} A, A \triangleleft (I_0, I_1)}{A \mid\equiv C \mid\sim (I_0, I_1)} \tag{7}$$

由初始假设式 (5) 和消息新鲜性推理规则可得:

$$\frac{A \mid\equiv \#(I_1)}{A \mid\equiv \#(I_0, I_1)} \tag{8}$$

由式 (7)、式 (8) 和临时校验规则可推出:

$$\frac{A \mid\equiv C \mid\sim (I_0, I_1), A \mid\equiv \#(I_0, I_1)}{A \mid\equiv C \mid\equiv (I_0, I_1)} \tag{9}$$

由式 (9) 和信仰规则可推出:

$$\frac{A \mid\equiv C \mid\equiv (I_0, I_1)}{A \mid\equiv C \mid\equiv I_1} \tag{10}$$

由初始假设条件式 (6) 与式 (10), 根据仲裁规则得:

$$\frac{A \mid\equiv C \Rightarrow I_1, A \mid\equiv C \mid\equiv I_1}{A \mid\equiv I_1} \tag{11}$$

证明结果显示, 协议可达到目标:

$$A \mid\equiv I_1$$

用户 A 相信从 CFL-CGC 证书生成中心返回证书的认证属性, 从而信任 CFL-CGC 的身份.

2.2 用户与验证设备的认证属性形式化分析

用户 A 将带有 CFL-CGC 证书的 UKey 插入验证设备, 由验证设备完成证书的验证后, 才能完成对用户 A 身份的信任. 设验证设备为 B.

步骤 1. 协议形式化:

$$A \rightarrow B : \{ID, sign_{ID}, sign_{IDSK}\} \tag{12}$$

$$B \rightarrow A : \{\text{TRUE/FALSE}\} \tag{13}$$

步骤 2. 初始假设:

$$B \mid\equiv \xrightarrow{IDPK} C \tag{14}$$

$$B \triangleleft \{ID\}_{IDSK} \tag{15}$$

$$B \mid\equiv C \Rightarrow ID \tag{16}$$

$$B \mid\equiv \#(ID) \tag{17}$$

步骤 3. 协议目标:

$$B \mid\equiv \#(ID)$$

步骤 4. 推理验证:

由初始假设式 (14) 和式 (15), 根据公钥消息含义推理可得:

$$\frac{B \mid\equiv \xrightarrow{IDPK} C, B \triangleleft \{ID\}_{IDSK}}{B \mid\equiv C \mid\sim ID} \tag{18}$$

由式 (18) 和初始假设式 (17), 根据临时值验证规则可得:

$$\frac{B \mid\equiv C \mid\sim ID, B \mid\equiv \#(ID)}{B \mid\equiv C \mid\equiv ID} \tag{19}$$

由式 (19) 和初始假设式 (16), 根据仲裁规则得:

$$\frac{B \mid\equiv C \mid\equiv ID, B \mid\equiv C \Rightarrow ID}{B \mid\equiv ID} \tag{20}$$

证明结果显示, 协议可达到目标: $B \mid\equiv ID$.

验证设备 B 完成对用户 A 的身份认证, 进而允许用户 A 对设备的设置及操作. 至此, 应用 BAN 逻辑分析完用户 A 对 CFL-CGC 的认证属性和验证设备 B 对用户 A 的认证属性[28], 本方案实现了安全目标, 用户与验证设备之间实现了安全的认证.

3 实验分析与测试

本节将从理论分析和实验测试 2 个方面对本文所提方案进行性能评估, 并与 PKI[8]方案, ECDSA[13]方案进行比较.

3.1 理论分析

3.1.1 通信开销

本节对比本文方案与 PKI[8]方案、ECDSA[13]方案的通信开销, 由于证书的签名和验证是两个不同时发生的阶段, 因此本文对两个阶段分开讨论. 注册阶段包括用户向 CGC 证书生成中心发送身份信息和请求, CGC 为用户端返回签名的证书; 验证阶段包括用户向验证端提供证书和验证端给用户返回验证结果[28]. 假设 RC 表示用户端与 CGC 间 1 次通信, RV 表示用户端与验证端 1 次通信, 表 1 为 3 种方案的通信开销对比.

表 1 通信开销对比

方案	注册阶段	验证阶段	总通信开销
PKI[8]	2RC	2RC+2RV	4RC+2RV
CFL	2RC	2RV	2RC+2RV
ECDSA[13]	4RC	4RV	4RC+4RV

由表 1 可知, 在注册阶段, PKI 方案与本文提出的 CFL 方案都有 2 次 RC 通信, ECDSA 方案有 4 次 RC 通信. 在验证阶段, PKI 方案除了 2 次 RV 通信, 还有 2 次 RC 通信, ECDSA 方案包括了 4 次 RV 通信, CFL 方案有 2 次 RV 通信. 在实际应用场景中,

一个用户在证书有效期内只会进行一次注册和无数次验证, 因此验证阶段的通信开销对证书生命周期的总开销来说是决定性的, 由表 1 可知, CFL 方案的通信开销比另外两种方案都具有优势.

3.1.2 计算开销

通过统计协议执行过程中使用的密码运算操作个数, 对 PKI 方案、ECDSA 方案和本文 CFL 方案的计算开销进行了理论分析与比较. 定义 H 为哈希运算, PM 为椭圆曲线点乘法运算, PA 为椭圆曲线点加法运算, RNG 为随机数产生. Kilinc 等[29]基于 PBC 库计算得出不同密码运算的平均耗时: H 约为 0.0023 ms, PM 约为 2.226 ms, PA 约为 0.0288 ms, RNG 约为 0.539 ms.

对比方案中的哈希运算 H 的总个数是在安全参数 256 的情况下进行统计的, 其中, ECDSA 方案中的 U1 和 U2 分别等价为证书生成中心和注册用户, 具体比较如表 2 所示.

由表 2 可知, 在注册阶段, CFL 方案算法由于涉及 2 次签名, 计算开销是 PKI 方案的 2 倍多; 对比 ECDSA 方案, CFL 方案减少了 3 次哈希运算, 7 次随机数运算, 增加了 1 次 PM 运算和 3 次 PA 运算. 在验证阶段, CFL 方案对比 PKI 方案略有增加, ECDSA 方案最慢.

表 2 各方案的计算开销对比

方案	注册阶段	验证阶段	总计算开销
PKI[8]	2H+2PM+1PA+RNG	4H+6PM+3PA+RNG	6H+8PM+4PA+2RNG
CFL	2H+7PM+3PA+2RNG	H+7PM+3PA	3H+14PM+6PA+2RNG
ECDSA[13]	5H+6PM+9RNG	8H+10PM	13H+16PM+9RNG

3.2 实验分析

3.2.1 工控系统仿真

温湿度是工业生产过程中一个重要的被控参数. 本文以环境温湿度监控系统作为工业控制系统仿真场景, 通过 LabVIEW 仿真平台实现. 平台使用 Proteus 进行电路仿真, 以 STC89C52 单片机作为主控制器, LCD 1602 显示温湿度, 温湿度传感器采用 DHT22, 外接除湿器和风扇进行温湿度控制. 硬件设计及上位机软件设计如图 6 和图 7 所示.

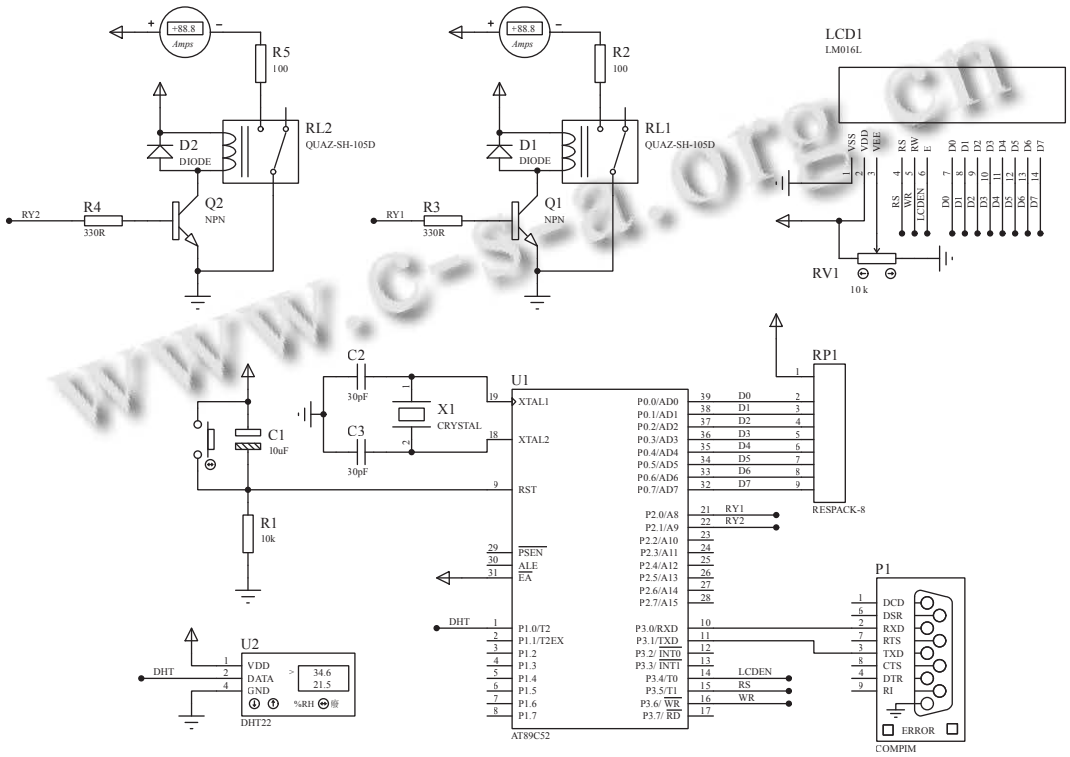

图 6 仿真电路原理图

图 7 环境温湿度监控系统设计界面

3.2.2 抗攻击测试实验

为了测试对比本方案防御 DoS 攻击的能力, 需要在实现的原型系统上进行 UDP-Flood 攻击实验, 攻击者通过恶意向目标工控设备发起认证响应请求, 并随机化源 IP 地址, 来消耗工控设备以及 CFL_CGC 的计算资源, 使其瘫痪. 测试工具采用 hping3, 分别对 3 种方案进行测试, 输出数据包响应时间, 然后统计出平均响应时间, 传输的数据包为 CFL 证书. 实验环境配置如表 3 所示.

表 3 抗攻击实验环境配置

参数	CFL_CGC	工控设备与终端	DoS攻击机
网络带宽 (Mb/s)	100	100	500
操作系统	Ubuntu	Ubuntu	Ubuntu
台数	4	10	1

在 DoS 攻击实验中, 各主机都处在同一个局域网中, 使用交换机相连, 攻击方式采用 UDP-Flood 方式, 实验测试了 3 种方案原型系统在不同 UDP-Flood 攻击速率下平均的请求认证服务响应时间以及各攻击速率下的系统可用性, 实验数据所绘折线图如图 8 所示.

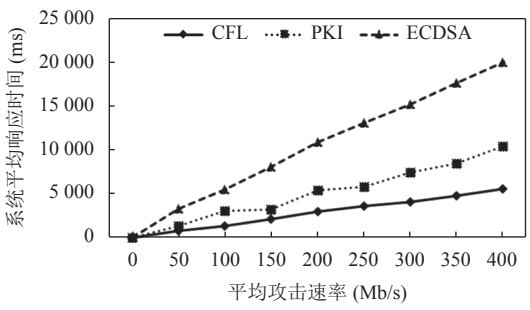

图 8 抗 DoS 攻击实验结果

实验结果表明, 本文方案的抗攻击特性优于其他两种方案, 且在攻击速率达到 400 Mb/s 时, ECDSA 方案出现了 20% 请求无法获得正确回应的情况. 本文方案最优的原因主要是, 只需要对证书进行验证即可, 即去中心认证, 所以大大减少了计算资源的消耗, 可以有效防御 DoS 攻击.

3.2.3 性能测试实验

在实验测试中, 本文以 NIST 标准化的 secp256k1 椭圆曲线为基准, 安全参数$\lambda = 256$, 杂凑函数采用 SM3, 签名和验证函数采用 SM2. 测试程序基于开源密码学库 Bouncy Castle 实现椭圆曲线上的计算, 使用 Java 语言编写, 基于 PC 端开发, 主要运行环境如表 4 所示.

表 4 服务器配置对比

配置	云服务器	CFL验证服务器
处理器	2核	2核
内存 (GB)	4	8
地点	北京	本地

数据库: MySQL

操作系统: Windows 7 旗舰版

UKey: Kingston DT100G3 (32 GB)

在不考虑网络延时的情况下, 我们分别测试 3 种方案在注册阶段和验证阶段的工作性能.

使用压力测试工具 Apache JMeter 在仿真工控系统注册和验证的场景下测试执行事务的效率, 其中设置种子秘钥长度为 128, 每一组数据均取 20 轮实验的平均值, 图 9 为系统注册吞吐量对比图, 图 10 为系统验证吞吐量对比变化图. 在证书注册阶段, 3 种方案的证书生成中心都部署在云服务器上, 通过图 9 可知, 随着注册用户个数的增加, PKI 和 CFL 方案的系统吞吐量变化并没有发生太大的波动, ECDSA 方案吞吐量随着注册用户量的增加而缓慢增加, PKI 方案与 CFL 方案几乎保持持平, 都高于 ECDSA 方案的吞吐量. 图 10 为证书验证阶段系统的吞吐量, 在验证用户个数为 100 个/s 时, CFL 方案的系统吞吐量比 PKI 方案提高了 676.62%, 在用户数为 400 个/s 时, CFL 方案的系统吞吐量比 ECDSA 方案也有大幅提高, 且在其他验证用户个数的情况下, 也明显高于另外两种方案, 体现出 CFL 方案在验证阶段吞吐量方面的优越性. 具体系统响应时间如图 11 和图 12 所示. 通过对比图 11 注册阶段 3 种方案的系统响应时间可知, ECDSA 方案随着注册用户数的增加系统响应时间增速最快, 并且都高于 CFL 方案和 PKI 方案, CFL 方案的响应时间略高于

PKI 方案. ECDSA 方案与 PKI 方案的系统响应时间都不断增加, CFL 方案系统响应时间增速和总时间都明显低于另外两种方案的时间, 并且可看出 CFL 方案系统验证响应时间能够满足毫秒级应用. 在工控系统身份认证现实场景中, 用户一般完成一次注册后会进行多次的验证, 即系统验证阶段的性能才能决定整体性能的好坏. 通过本文的实验测试结果可知, 当证书中心的注册系统和验证系统分开后, 本文所提的 CFL 工控系统认证方案因为在验证阶段系统整体性能吞吐量大, 响应时间短, 提高了系统处理事务的效率, 更适合工控系统的大规模身份认证.

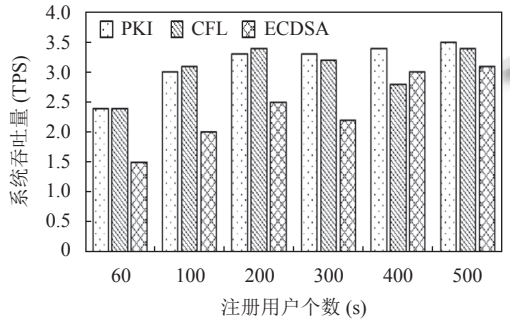

图 9 系统注册吞吐量

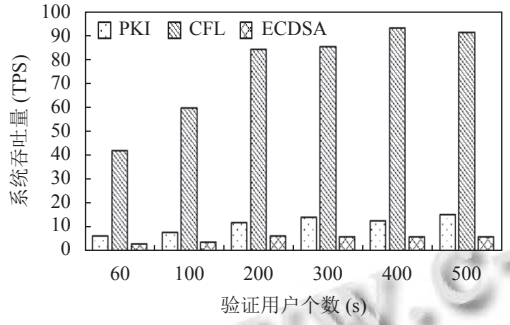

图 10 系统验证吞吐量

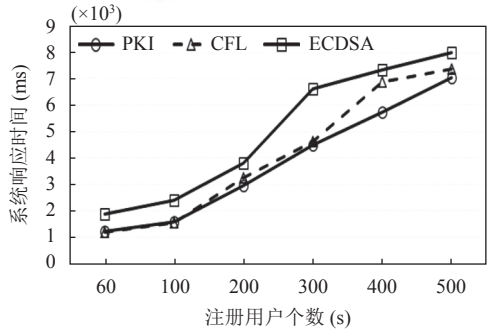

图 11 系统注册响应时间

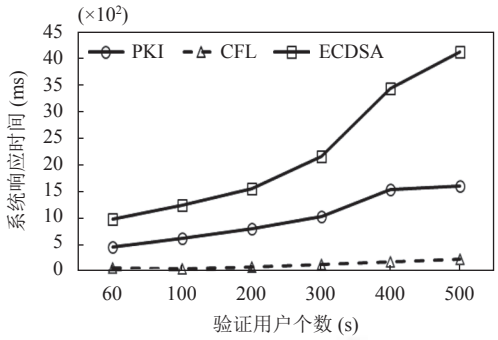

图 12 系统验证响应时间

4 结论

工业控制系统身份认证的安全性和工作效率日益受到国际社会的关注, 针对当前身份认证系统中心化程度过高以及用户对私钥私有权的强烈需求. 本文利用国内学者提出的 CFL 认证体制提出了基于 CFL 的工控系统签名方案, 并建立了工控系统认证模型 CFL-SYS. 同时引入 UKey 作为证书的载体, 通过计算 ID 的哈希值生成验证公钥, 实现了验证阶段的去中心化, 减轻了证书中心的压力, 提高了系统吞吐量, 降低了系统响应时间. 然后使用 BAN 逻辑分析证明本文方案的安全性和可行性, 最后通过对比实验测试表明, 本文方案在性能方面相比 PKI 方案, ECDSA 方案具有优势, 能够为大规模的工业控制系统提供一种自主、可靠、高效的身份认证.

参考文献

1 王震, 范佳, 成林, 等. 可监管匿名认证方案. 软件学报, 2019, 30(6): 1705–1720. [doi: 10.13328/j.cnki.jos.005746]

2 NIST. Federal agency use of public key technology for digital signatures and authentication. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151224. (2000-10-01).

3 Camenisch J, Lysyanskaya A. Signature schemes and anonymous credentials from bilinear maps. Proceedings of the 24th Annual International Cryptology Conference on Advances in Cryptology. Santa Barbara: Springer, 2004. 56−72.

4 Boneh D, Boyen X, Shacham H. Short group signatures. Proceedings of the 24th Annual International Cryptology Conference on Advances in Crypto Crypto. Santa Barbara: Springer, 2004. 41−55.

5 王中华, 韩臻, 刘吉强, 等. 云环境下基于 PTPM 和无证书公钥的身份认证方案. 软件学报, 2016, 27(6): 1523–1537.

[doi: 10.13328/j.cnki.jos.004992]
6 Hardjono T, Smith N, Pentland A. Anonymous identities for permissioned blockchains. https://petertodd.org/assets/2016-04-21/MIT-ChainAnchor-DRAFT.pdf. (2016-04-21).
7 Ye QQ, Tan HC, Mashima D, *et al*. Position paper: On using trusted execution environment to secure COTS devices for accessing industrial control systems. Authorea Preprints, 2023.
8 魏珊珊, 韩庆敏, 郭肖旺, 等. 基于国密算法的 PKI 在工控系统中的应用研究. 计算机与现代化, 2018(11): 1–6. [doi: 10.3969/j.issn.1006-2475.2018.11.001]
9 Mackenzie P, Reiter MK. Two-party generation of DSA signatures. International Journal of Information Security, 2004, 2(3-4): 218–239. [doi: 10.1007/s10207-004-0041-0]
10 Lindell Y. Fast secure two-party ECDSA signing. Journal of Cryptology, 2021, 34(4): 44. [doi: 10.1007/s00145-021-09409-9]
11 Doerner J, Kondi Y, Lee E, *et al*. Secure two-party threshold ECDSA from ECDSA assumptions. Proceedings of the 2018 IEEE Symposium on Security and Privacy. San Francisco: IEEE, 2018. 980–997.
12 Castagnos G, Catalano D, Laguillaumie F, *et al*. Two-party ECDSA from hash proof systems and efficient instantiations. Proceedings of the 39th Annual International Cryptology Conference on Advances in Cryptology. Santa Barbara: Springer, 2019. 191–221.
13 王婧, 吴黎兵, 罗敏, 等. 安全高效的两方协同 ECDSA 签名方案. 通信学报, 2021, 42(2): 12–25.
14 He DB, Zhang YD, Wang D, *et al*. Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography. IEEE Transactions on Dependable and Secure Computing, 2020, 17(5): 1124–1132. [doi: 10.1109/TDSC.2018.2857775]
15 侯红霞, 杨波, 张丽娜, 等. 安全的两方协作 SM2 签名算法. 电子学报, 2020, 48(1): 1–8. [doi: 10.3969/j.issn.0372-2112.2020.01.001]
16 Zhang YD, He DB, Zhang MW, *et al*. A provable-secure and practical two-party distributed signing protocol for SM2 signature algorithm. Frontiers of Computer Science, 2020, 14(3): 143803. [doi: 10.1007/s11704-018-8106-9]
17 中华人民共和国国家质量监督检验检疫总局, 中国国家标准化管理委员会. GB/T 32918.2-2016 信息安全技术 SM2 椭圆曲线公钥密码算法第 2 部分: 数字签名算法. 北京: 中国标准出版社, 2017.
18 汪朝晖, 张振峰. SM2 椭圆曲线公钥密码算法综述. 信息安全研究, 2016, 2(11): 972–982.
19 陈华平, 范修斌, 吕述望. 基于标识的证书认证体制 CFL: 中国, 102957536B. 2016-02-17.
20 王海平, 王瑜, 李有文, 等. 典型信息安全 CFL 解决方案. 信息安全研究, 2016, 2(7): 639–648.
21 刘文婷, 杜春玲, 范修斌, 等. CFL 密钥管理研究. 信息安全研究, 2016, 2(7): 628–638.
22 舒展翔, 李腾飞, 余祥, 等. 基于 CFL 认证体制的区块链系统认证机制研究. 计算机应用研究, 2021, 38(2): 347–355.
23 王琳, 王夕冉, 侯博文, 等. 基于 CFL 的空间网络认证策略研究. 计算机应用研究, 2022, 39(11): 3455–3460.
24 郭旭. USB key 身份认证产品的产生与发展. 网络安全技术与应用, 2022(1): 31–32.
25 Wang GQ, Cao YM. An efficient certificate-based signature scheme in the standard model. Proceedings of the 19th International Conference on Applied Cryptography and Network Security. Kamakura: Springer, 2021. 313–329.
26 Camenisch J, Dubovitskaya M, Enderlein RR, *et al*. Concepts and languages for privacy-preserving attribute-based authentication. Journal of Information Security and Applications, 2014, 19(1): 25–44. [doi: 10.1016/j.jisa.2014.03.004]
27 Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems. Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali. ACM, 2019. 203–225.
28 Wang CY, Wang D, Xu GA, *et al*. Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0. Science China Information Sciences, 2022, 65(1): 112301. [doi: 10.1007/s11432-020-2975-6]
29 Kilinc HH, Yanik T. A survey of SIP authentication and key agreement schemes. IEEE Communications Surveys & Tutorials, 2014, 16(2): 1005–1023.

(校对责编: 张重毅)