信息与控制　2019 年　第 48 卷　第 3 期：344 ~ 353

DOI：10.13976/j.cnki.xk.2019.8539　　文章编号：1002 - 0411(2019) - 03 - 0344 - 10

面向工业控制系统终端的轻量级组认证机制

尚文利[1,3,4,5]，杨路瑶[1,2,4,5]，陈春雨[1,2,3,5]，尹　隆[1,3,4,5]，曾　鹏[1,3,4,5]，刘周斌[1,3,4,5]

1. 中国科学院沈阳自动化研究所，辽宁 沈阳　110016；　2. 东北大学信息科学与工程学院，辽宁 沈阳　110004；
3. 中科院网络化控制系统重点实验室，辽宁 沈阳　110016；　4. 中国科学院大学，北京　100049；
5. 中国科学院机器人与智能制造创新研究院，辽宁 沈阳　110016

基金项目：国家重点研发计划项目(2018YFB2004200)；中科院战略性先导科技专项(XDC2020200)；国家自然科学基金资助项目(61773368)；国家电网公司科技项目(52110118001H)

通信作者：尚文利，shangwl@sia.cn　收稿/录用/修回：2018 - 10 - 30/2019 - 03 - 11/2019 - 04 - 12

摘要

针对当前国内工控系统中普遍缺乏认证能力的现状，本文结合无证书签名和传统信息安全中的群组认证提出了一种面向工控终端的轻量级组认证机制，针对传统信息安全中的身份认证技术进行改进，实现工控系统中多机协作场景下对多台 PLC 进行同时认证. 基于本方案实现的可信 PLC 设备采用嵌入式处理器和安全处理单元的结构，在数据传输时采用 PCIE 协议传输，替代了传统的网络接口的数据传输，确保网络数据不会外泄，最大程度上保证了数据的安全性. 验证表明，本文提出的轻量级组认证机制减少了认证过程的计算量和通信开销，能够解决控制系统中身份认证机制存在的终端计算能力有限等问题.

关键词

无证书签名
组认证机制
PCIE 协议
安全处理单元

中图法分类号：TP301

文献标识码：A

Lightweight Group Authentication Mechanism for Industrial Control System Terminals

SHANG Wenli[1,3,4,5], YANG Luyao[1,2,4,5], CHEN Chunyu[1,2,3,5], YIN Long[1,3,4,5], ZENG Peng[1,3,4,5], LIU Zhoubin[1,3,4,5]

1. *Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang* 110016, *China*;
2. *School of Information Science and Engineering, Northeastern University, Shenyang* 110004, *China*;
3. *Key Laboratory of Network Control System of Chinese Academy of Sciences, Shenyang* 110016, *China*;
4. *Universityof Chinese Academy of Sciences, Beijing* 100049, *China*;
5. *Institudes for Robotics and Intelligent Manufacturing, Chinese Academy of Sciences, Shenyang* 110016, *China*

Abstract

Aiming at the current lack of certification ability in domestic industrial control system, we propose a lightweight group authentication mechanism for industrial control terminal; the mechanism combines the group authentication method of uncertificated signature and traditional information security. The proposed scheme improves the identity authentication technology in traditional information security and realizes simultaneous authentication of multiple PLCs in the multi-machine collaboration scenario of the industrial control system. The structure of the reliable PLC device based on the scheme adopts the embedded processor and the security processing unit. In this scheme, the PCIE protocol is used to transmit data, instead of the traditional network interface data transmission. It can certificateless signature group authentication mechanism. The PCIE protocol security processing unit ensures that network data are not compromised and that data security is guaranteed to the greatest extent. The verification shows that the proposed lightweight group authentication mechanism reduces the computational complexity and communication overhead of the authentication process. It can solve the problem of limited computing power of the terminal in the control system.

Keywords

certificateless signature;
group authentication mechanism;
PCIE protocol;
security processing unit

0　引言

当前，随着信息和互联网技术的高速发展以及它们向各产业的不断延伸与渗透，原有封闭、孤立的工业控制系统逐步走向开放、互联，一个高度自动化、个性化和互动化的工业互联网即将诞生. 互联网技术为工业控制领域带来了技术进步、生产率提高与竞争实力大大增强的利益，然而在工业控制领域享受这些利益的同时，也面临着越来越严峻的信息安全挑战，病毒、木马等威胁正在向工业控制系统扩散[1-2].

对于工业控制系统的攻击手段，主要分为对工业企业数据的攻击、对控制性能的攻击、对控制功能的攻击，近几年工业控制系统遭到攻击的恶性事件层出不穷，自 1982 年在苏联发现的首个 SCADA 逻辑炸弹，到 2010 年伊朗核电站“震网”事件，再到 2016 年亚洲能源行业“洋葱狗”等事件均表明网络安全威胁的触角已真正地开始向工业领域蔓延. 工业控制系统一旦遭到破坏，会造成整个控制系统的工作异常，控制器失灵，数据信息遭到窃取与破坏，这不仅会影响产业经济的持续发展，更会对国家安全造成巨大的损害，总而言之当前工业控制系统的信息安全形势十分严峻[3-4].

目前，工业测控系统的核心仍然是以 PLC 为代表的可编程嵌入式电子设备，但其自身安全防护能力较弱，认证机制和访问控制的防护不足，很容易遭到入侵，进而对整个系统造成破坏. 工业控制系统一旦遭到破解，则可能造成工业控制中的控制 PLC 启停、植入恶意 PLC 逻辑与自定义固件等高危持续性威胁[5]，后果不堪设想，这已经成为影响我国工控系统安全的重要问题. 基于密码技术保护工控网络中数据传输的机密性、完整性和不可否认性成为越来越重要的技术手段. 所以加强工业控制系统信息安全的防护，采用密码技术解决工控系统信息安全问题是大势所趋[6].

作为通信网络环境下的一种安全保密基础设施，身份认证机制一直都是密码技术中重要的研究方向. 认证机制作为工业控制系统信息安全防护的一道重要关卡，不仅可以有效地阻挡非法用户对工控系统的未授权访问，同时群组认证还可以用来检测多个终端中是否存在已被入侵的终端，进而保护系统的敏感资源. 在工控系统中添加密码学中的认证模块可以为工控系统提供或增强身份认证的能力，确保工控网络中数据传输的机密性与安全性. 所以迫切需要将一种完整高效的认证机制应用到工控场景中[7].

1　国内外研究现状

典型的工业控制系统，一般分为现场控制层、监控管理层、企业管理层三层. 现场设备层主要由负责工业制造的设备、仪器仪表、传送设备等物理设施组成，现场设备通过现场总线或者工业以太网与工业控制终端进行连接，PLC 或 RTU 设备负责实现局域控制功能；监控管理层主要由上位机、数采机、数据服务器、HMI 组成，并由 OPC、工业以太网等进行通讯，主要负责对相应的控制器以及物理设备等参数的设定与控制，以及实时数据的上传与监控；企业管理层主要由相应的管理终端通过以太网进行通讯，负责生产过程的管理、生产计划制定等[8]. 随着互联网的发展，现场控制层、监控管理层和企业管理层，这三层之间的通讯逐渐开始与企业网、因特网互联. 其中现场设备层中的数据最为重要，其核心设备是以 PLC 为代表的可编程嵌入式电子设备，因此 PLC 设备面临的网络安全风险也随之增大. 针对 PLC 产品与其他设备交互时认证技术不完善等相关问题，国内外一些学者提出了相应的改进办法.

Hayes 等人提出一种基于哈希运算消息认证码(HMAC)和流控制传输协议(SCTP)技术的后向兼容 Modbus改进安全协议 Modbus Sec，其可为系统提供可靠的消息传递服务，并实现设备间的双向认证，但是该方案的安全性过分依赖于其预共享密钥的长度和复杂性，该方案缺乏实用性[9]. Morris 等人提出一种改进的入侵检测软件 Modbus RTU/ACSII Snort，将串行连接流量转换为以太网 TCP/IP 流量进行传输和检测，该入侵检测软件未做通讯实时性、有效性的测试，对通讯实时性、有效性要求比较苛刻的环境没有保证[10]. 信息安全界对工业控制系统中终端设备和网络的接入安全也进行了研究. TCG 组织于 2014 年将可信计算技术引入 ICS，利用可信度量和可信连接为 ICS 的终端、网络等提供更高级别的安全保护，但这种方案只改进了终端设备和网络接入的安全，并未改进终端设备通信使用的协议，存在一定的安全隐患，如通信报文被窃听[11]. 杨静等人针对 Modbus/TCP 协议缺乏身份认证，提出一种新的 Modbus/TCP 协议安全增强方法，可以完成通信双方的认证，但数据处理耗时较大，不满足实时性要求[12]. 王勇等人提出基于可信计算的身份认证方法，采用基于数字证书的身份认证方法，构建了可信 PLC 的安全认证模型，但是该方法计算量大，认证过程较为繁琐[13].

针对上述实用性差、安全性低和计算量大等问题，本文针对传统信息安全中的身份认证技术进行了改进，并将改进后的认证技术应用到工业控制系统中，实现了工控系统中多机协作场景下对多台 PLC 进行同时认证的功能，便于多个终端同时管理，提高系统的认证效率，增强整个系统的安全性与可靠性，解决控制系统中身份认证机制存在的认证过程繁琐终端计算能力有限等问题.

2　相关理论基础

2.1　密码学相关理论基础

2.1.1　无证书签名机制

无证书签名机制通常由以下 7 个算法组成[14-15]：

1)系统建立

这个算法由密钥生成中心(KGC)完成. 算法输入参数 1^k，输出主密钥 s 和系统参数 params. KGC 保密 s，公开 params. 这里 k 是一个安全参数.

2)部分私钥提取

这个算法生成用户的部分私钥，由 KGC 完成. 算法输入一个用户的身份 ID_U，KGC 计算该用户的部分私钥并通过安全方式发送给这个用户.

3)设置秘密值

该算法输入系统参数 params 和一个用户的身份 ID_U，输出该用户的秘密值 x_U.

4)设置私钥

该算法输入系统参数 params 和一个用户的部分私钥 D_U 与秘密值 x_U，输出一个完全的私钥 S_U.

5)设置公钥

该算法输入系统参数 params 和一个用户的秘密值，输出该用户的公钥 PK_U.

6)签名

该算法输入系统参数 params、一个签名者的身份 ID_U 与公钥 PK_U、一个签名者的私钥 S_U 和一个消息 m，输出一个签名 σ.

7)验证

该算法输入系统参数 params，一个签名者的身份 ID_U 与公钥 PK_U、一个消息 m 和一个签名 σ，输出“真”(表示签名 σ 对于消息 m 和(ID_U,PK_U)是合法的)或者“伪”(表示签名 σ 对于消息 m 和(ID_U,PK_U)是不合法的).

2.1.2 Shamir 门限方案

1979 年，Shamir 提出了一个基于多项式拉格朗日插值的(k, n)门限方案. 设 p 为一个素数，$p \geq n+1$，共享秘密 $s \in Z_p$. 假设由一个可信中心 T 来给这 n 个用户分配秘密份额，Shamir 门限方案由份额分配算法和恢复算法构成[16-17].

1)份额分配算法

(i)T 随机选择 $k-1$ 个独立的系数 $a_1, a_2, \cdots, a_{k-1} \in Z_p$，定义 $a_0 = s$，建立一个多项式：

$$f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$$

(ii)T 选择 n 个互不相同的元素 $x_1, x_2, \cdots, x_n$

$x_{k-1} \in Z_p$，并计算 $y_i = f(x_i) \bmod p$，$1 \leqslant i \leqslant n$. 最直接的方法是令 $x_i = i$.

(iii)将(x_i,y_i)分配给用户 U_i，$1 \leqslant i \leqslant n$,其中 x_i 公开，y_i 为 U_i 的秘密份额.

2)恢复算法

任何 k 个或更多的用户将他们的份额集中起来. 这些份额提供了 k 个不同的点(x_i,y_i)，可以通过拉格朗日插值计算出 $f(x)$ 的系数 a_i. $1 \leqslant i \leqslant k-1$. 秘密 s 就可以通过计算 $f(0) = a_0 = s$ 得到.

对于一个次数小于 k 的未知多项式 $f(x)$ 来说，给定 k 个点(x_i,y_i),$1 \leqslant i \leqslant k$，我们就可以根据拉格朗日插值公式进行重建：

$$f(x) = \sum_{i=1}^{k} y_i \prod_{j=1, j \neq i}^{k} \frac{x - x_i}{x_i - x_j}$$

既然 $f(0) = a_0 = s$，共享的秘密可以表示成

$$s = \sum_{i=1}^{k} c_i y_i$$

其中，$c_i = \prod_{j=1, j \neq i}^{k} \frac{x - x_i}{x_i - x_j}$，既然 c_i 是公开的，这 k 个用户都可以计算出秘密信息 s.

2.2 工控网络相关理论基础

2.2.1 TPM 安全芯片

可信平台模块(Trusted Platform Module)是一种植于计算机内部为计算机提供可信根的芯片. TPM 是一个含有密码运算部件和存储部件的小型片上系统，它由 CPU、存储器、I/O、密码运算器、随机数产生器和嵌入式操作系统等部件组成. 它是具有加密功能的安全微控制器，旨在提供涉及加密密钥的基本安全功能.

TPM 安全芯片，是指符合 TPM 标准的安全芯片，它能有效地防止非法用户访问，可实现数据加密、密码保护等安全功能. 它所起的作用相当于一个“保险柜”，最重要的密码数据都存储在安全芯片中，安全芯片配合管理软件完成各种安全保护工作，而且根据安全芯片的原理，由于密码数据只能输出，而不能输入，这样加密和解密的运算在安全芯片内部完成，而只是将结果输出到上层，避免了密码被破解的机会[18].

2.2.2 PCI-e 总线概述

PCI-Express(又称 PCI-e)是一种高性能、高带宽串行通讯互联标准，它取代了基于总线的通信构架，如：PCI、PCI Extended(PCI-X)以及加速图形端口(AGP). PCI-e 具有更低的生产成本、更高的系统吞吐量和更好的可扩展性与灵活性等主要性能.

随着现代处理器技术的发展，在互连领域中，使用高速差分总线替代并行总线是大势所趋. 与单端并行信号相比，高速差分信号可以使用更高的时钟频率，从而使用更少的信号线，完成之前需要许多单端并行数据信号才能达到的总线带宽. PCIE(Peripheral Comp-onent Interconnect-Express)总线使用了高速差分总线，并采用端到端的连接方式，因此在每一条 PCIE 链路中只能连接两个设备. PCIE 总线使用了一些在网络通信中使用的技术，如支持多种数据路由方式、基于多通路的数据传递方式和基于报文的数据传送方式，并充分考虑了在数据传送中出现服务质量 QoS(Quality of Service)问题[19].

3 轻量级组认证机制

3.1 符号描述

本文结合无证书签名机制和传统信息安全中的群组认证方案，提出了面向工控终端的轻量级组认证机制. 本文中的机制在秘密份额传输时使用了 CLSC(cer-tificateless-signcryption)机制，用来解决第三方的不可信问题，防止其下发假的份额给终端. 同时，该机制可以在全部 n 台 PLC 中，对其中任意 $m(t \leqslant m \leqslant n)$台 PLC 进行整体组认证，判断 m 台参与认证的 PLC 是否都处于安全通信的状态，该机制主要为以 PLC 为核心的工控系统添加认证机制，增强整个系统的安全性与可靠性. 本文中的机制所涉及到的符号描述如表 1 所示.

表 1　符号描述

Tab.1　Symbol description

符号	描述
U	工程师站与 PLC 标识的集合
x_i	公开身份信息 ID
k	系统的安全参数
s^*	系统主密钥
pp	系统公开参数
G_1，G_2，G_T	构造双线性映射的循环群
p，q，g	分别为 G_1，G_2，G_T 的生成元
φ	同构函数
e	双线性对映射函数
P_{pub}	系统的公钥
H_1，H_2，H_3	3 个不同的加密哈希函数
n	被签名消息的长度
p，q	大素数(p 是 G_1，G_2，G_T 的阶)
d_{xi}	部分私钥
Q_{xi}，T_{xi}	计算密钥产生的中间值
x_{xi}	秘密值
sk_{xi}	私钥
pk_{xi}	公钥
s	总的秘密值
s_i	秘密份额
a_i	随机多项式 f 的系数
$H(s)$	验证阶段使用的单项哈希函数
r_i	随机选取的计算值
c，u，v，w	构成签名的 4 个计算值
δ	签名
g^{r1}，h_2	计算签名产生的中间计算量
P	参与认证的 PLC 标识的集合
C_i	随机分量
s'	参与认证的 PLC 计算出的秘密值

注：论文中涉及上述符号且下标后缀有 s(send)的为发送方，有 r(receive)的为接收方.

3.2　认证实体

本文中的机制包括系统中的 PLC 设备、工程师站和密钥生成服务器，认证实体的具体描述如下：

1)系统中的 PLC 设备：为系统中的 PLC 设备添加 PCIE 网络安全单元，并使用具有身份认证功能的可信 PLC 控制器作为系统中的主控设备，构成安全可信的认证环境. 系统中所有的 n 台可信 PLC 都会在工程师处成功注册并获得有效的秘密份额. 但是，在认证阶段只有 m 台参与认证的可信 PLC 会生成随机分量进行组内认证.

2)工程师站：工程师站在本机制中负责选择多项式的参数和秘密值、计算并公开秘密的 Hash 值、生成秘密份额并通过无证书签名方式安全地分发给可信 PLC 主控，并且在认证阶段负责判断可信 PLC 主控最终计算出的秘密的 Hash 值是否正确.

3)密钥生成服务器：密钥生成服务器在本机制的主要工作是设置并发布系统的公开参数，提取工程师站和所有可信 PLC 的部分私钥，并将提取到的相应的部分私钥发送到工程师站和系统中所有的可信 PLC 中，在整个机制的过程中该步骤仅执行一次.

数据信息的实体交互图如图 1 所示.

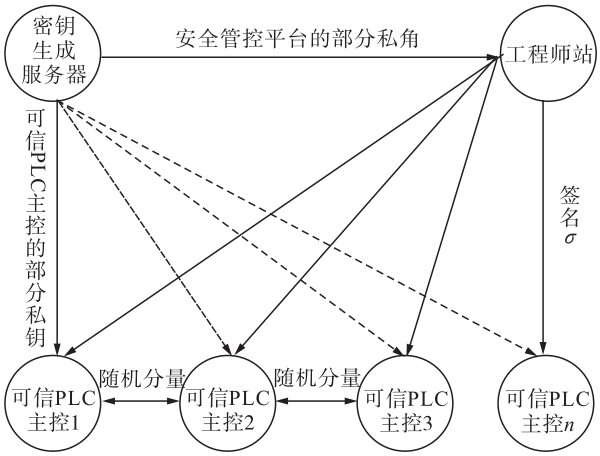

图 1　实体信息交互图

Fig.1　Entity information interaction map

3.3　认证流程

在整个机制中，先由密钥生成服务器进行一系列的准备工作，包括给定双线性配对组、选取系统主密钥和选择 3 个不同的加密哈希函数等. 之后密钥生成服务器计算并公开系统参数，以及提取出所有可信 PLC 主控和工程师站的部分私钥，并将部分密钥下发，机制的通信过程也由此开始. 所有可信 PLC 主控和工程师站接收到相应的部分私钥后根据各自的身份信息 ID 和系统的公开参数生成自己的公钥和完整的私钥.

当上述的准备工作一切就绪之后，工程师站开始选择秘密值 s、随机多项式 f 和单项哈希函数 $H(s)$，再根据系统中每台可信 PLC 主控的身份信息 ID 计算它们相应的秘密份额 s_j. 之后，工程师站利用无证书签名的方式将相对应的秘密份额安全地发送给每台可信 PLC 主控. 可信 PLC 主控接收到签名后使用自己的身份信息 ID、工程师站的公钥和自己的私钥对签名进行验签. 如果签名有效则根据接受到的秘密份额进行组内认证，否则丢弃接受到的秘密份额，等待下一次的秘密份额发送.

在确认过签名有效后，参与认证的 $m(t \leqslant m \leqslant n)$ 台可信 PLC 主控开始进行组认证. 参与认证的 m 台可信 PLC 主控根据接受到的秘密份额生成各自相应的随机分量，之后每一台可信 PLC 向其他参与认证的可信 PLC 发送随机分量，当接收到所有的随机分量后，开始组内的认证过程.

每台参与认证的可信 PLC 通过恢复出来的秘密值 s' 计算 $H(s')$，可信 PLC 主控将 $H(s')$ 发送到工程师站，工程师站再通过判断是否成立来判定 $H(s') = H(s)$ 是否存在非法的 PLC 设备. 如果认证结果成立，工程师站和 PLC 设备之间则可以开始正常的数据通信. 如果认证结果不成立，则说明参与认证的 PLC 设备中存在可疑的 PLC 设备参与到了认证的过程中，企图加入组内，获取工业控制系统过程中的相关数据，此时相关的工作人员应该提高警惕，开

始一系列的排查工作，整个机制的流程图如图 2 所示.

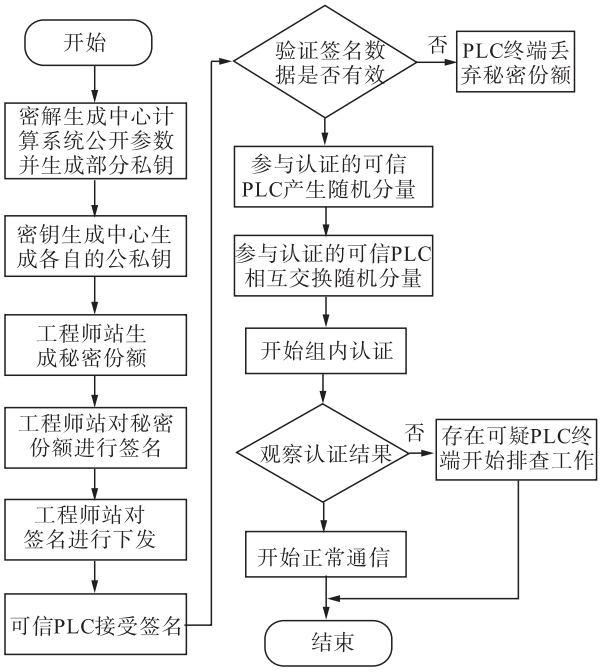

图 2 流程图

Fig.2 Flow chart

3.4 认证步骤

3.4.1 准备阶段

在准备阶段由 3 个算法组成，分别是初始化算法、部分私钥提取算法和设置公私钥算法，即Preparation-Phase = (Init, PartPKGet, Pri/PubKSet)，具体描述如下：

假设整个工控系统中共有 n 台可信 PLC 互连互通进行认证和一个工程师站，通过 $U=\{U_i \mid i=1, 2, \cdots, n, n+1\}$ 对这 n 台可信 PLC 和工程师站进行标识，每台可信 PLC 和工程师站(即 U_i)获取自己的设备编号记为 x_i，将 x_i 作为 U_i 的公开身份信息 ID 且 $x_i \neq 1$，其中，$i=1, 2, \cdots, n, n+1$.

1) $(s^*, pp) \leftarrow \text{Init}(k)$：初始化算法由密钥生成中心完成，算法输入一个安全参数 k，输出系统主密钥 s^* 和系统参数 params，密钥生成中心保密 s^*，公开 params，算法详细流程如下：

(i) 选取具有相同阶 p(其中 $p>2^k$)的循环(G_1, G_2, G_T)，其中群 G_1 和群 G_2 具有同构性，即 $\phi: G_2 \rightarrow G_1$，双线性配对函数为 $e: G_1 \times G_2 \rightarrow G_T$.

(ii) 选取 G_2 的任意生成元 Q，并设置 $P=\varphi(Q)$和$g=e(P,Q)$，使 P、g 分别是 G_1 和 G_2 生成元.

(iii) 随机选取系统主秘钥，$s^* \in RZ_p^*$，并将 $P_{\text{pub}}=s^*Q$设置为系统的公钥.

(iv) 选取 3 个不同的加密哈希函数 $H_1: \{0,1\}^* \rightarrow Z_p^*$，$H_2: \{0,1\}^n \times G_2 \times G_T \times G_2^3 \rightarrow Z_p^*$ 和 $H_3: G_2 \times G_T \rightarrow \{0,1\}^n$.

发布系统参数：$pp=<G_1, G_2, e, p, P, Q, g, P_{\text{pub}}, \varphi, H_1, H_2, H_T>$.

2) $(d_{xi}) \leftarrow \text{PartPKGet}(pp, s, x_i)$：部分私钥提取算法由密钥生成中心完成，算法输入身份信息 x_i，系统参数 pp 和系统主秘钥 s^*，输出每台可信 PLC 和工程师站的部分私钥，具体计算公式如下：

$$Q_{xi}=H_1(x_i) \in Z_p^* \tag{1}$$

$$d_{xi}=\frac{1}{s^*+Q_{xi}}P \tag{2}$$

参与认证的可信 PLC 和工程师站获取到相应的部分私钥后，通过计算：

$$e(d_{xi}, P_{\text{pub}}+Q_{xi}Q)=g \tag{3}$$

来确认所获取的部分私钥是否真实. 为了书写简便，在此定义：

$$T_{xi}=P_{\text{pub}}+H_1(x_i)Q \tag{4}$$

3) $(sk_{xi}, pk_{xi}) \leftarrow \frac{\text{Pri}}{\text{PubKSet}}(pp: x_i, d_{xi})$：设置公私钥算法由每台可信 PLC 和工程师站独自完成，该算法首先输入公开参数 pp 和身份信息 x_i，输出一个随机值作为秘密值 $x_{xi} \in RZ_p^*$，再输入公开参数 pp，身份信息 x_i 及其秘密值 x_{xi}，输出其公钥，具体计算公式如下：

$$pk_{xi}=x_{xi}(P_{\text{put}}+H_1(x_i)Q)=x_{xi}T_{xi} \tag{5}$$

之后再输入 pp，部分私钥 d_{xi}及其秘密值 $x_{xi} \in RZ_p^*$，输出一对(d_{xi}, x_{xi})作为每台可信 PLC 和工程师站的私钥 sk_{xi}.

该阶段的 UML 时序图如图 3 所示.

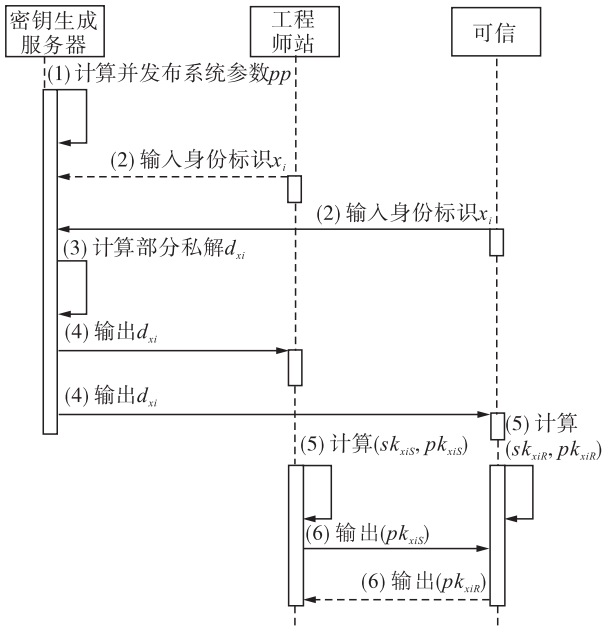

图 3 准备阶段时序图

Fig.3 Phase sequence diagram of preparation stage

3.4.2 注册阶段

在注册阶段由 3 个算法组成，分别是秘密份额生成算法，秘密份额下发算法和验签算法，Registration-Phase (ShaCre, ShaDis, ShaVer)，具体描述如下：

1) $(s, s_i) \leftarrow \text{ShaCre}(x_i)$：秘密份额生成算法由工程师站执行，该算法输入所有可信 PLC 的公开身份信息 x_i，输出秘密 s 的单项哈希值 $H(s)$和秘密份额 s_i，其中 $i=1, 2,$

…，n. 工程师站在该阶段为每台可信 PLC 生成一个门限秘密共享中的秘密份额 s_i，具体算法如下：

首先，工程师站选择两个大素数 p 和 q，使得 $p>q+nq^2$. 之后，在 GF(p)上随机选择 $t-1$ 个值 $a_i(i=1,2,\cdots,t-1)$，并在 GF(p)上选择 a_0 作为秘密 s，生成一个 $t-1$ 次随机多项式：

$$f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}\bmod p \tag{6}$$

其中，秘密 $s=a_0=f(0)$，然后工程师站利用每一台可信 PLC 的公开身份信息 x_i 计算 $f(x_i)$，并将其记为秘密份额 s_i.

2) ShaDis(sk_{xiS}, x_{iR}, pk_{xiR}, s_i)：秘密份额下发算法由工程师站执行，首先对一个秘密份额消息 $s_i\in\{0,1\}^n$ 进行签密，然后将签名发送给要接收消息的可信 PLC，具体计算公式如下：

随机选取 $r_i\in RZ_p^*$，计算下面给出的4 个值(c, u, v, w)：

(ⅰ) $c=s_i\oplus H_3(g^{r1}, r_1pk_{xiR})$ (7)

(ⅱ) $u=r_1(P_{\text{pub}}+H_1(x_{iR})Q)$ (8)

(ⅲ) $h_2=H_2(s_i, u, g^{r1}, r_1pk_{xiR}, pk_{xiR})$ (9)

$$v=\frac{r_1+h_2}{r_1}d\,xiS \tag{10}$$

(ⅳ) $w=x_{xis}h_2+r_1$ (11)

此时，设置签名 $\sigma=(c,u,v,w)$.

3) ShaVer(x_{iS}, pk_{xiS}, sk_{xiS},σ)：验签算法由可信 PLC 执行，对工程师站发送过来的签名 σ 进行验签，具体计算步骤如下：

(ⅰ)首先通过以下两个公式计算 $g^{r1'}$ 和 s_i 的值：

$$g^{r1'}=e(d_{xiR}, u) \tag{12}$$

$$s_i=c\oplus H_3(g^{r1'}, x_{xiR}u) \tag{13}$$

(ⅱ)然后通过以下两个公式设置 h_2 和 r'_1T_{xis}的值：

$$h_2=H_2(s_i, u, x_{xiR}u, pk_{xiS}, pk_{xiR}) \tag{14}$$

$$R'_1T_{xis}=wT_{xis}-h_2pk_{xiS} \tag{15}$$

(ⅲ)最后通过判断以下等式是否成立.

$$e(v_1+r'_1T_{six})=g^{r1'}g^{h2} \tag{16}$$

当且仅当等式成立时才接受 x_i，否则返回错误符号⊥(表示解密失败). 当解密失败时，说明该工程师站发送来的消息不可信，这时 PLC 终端会丢弃接受到的秘密份额，等待下一次的秘密份额发送.

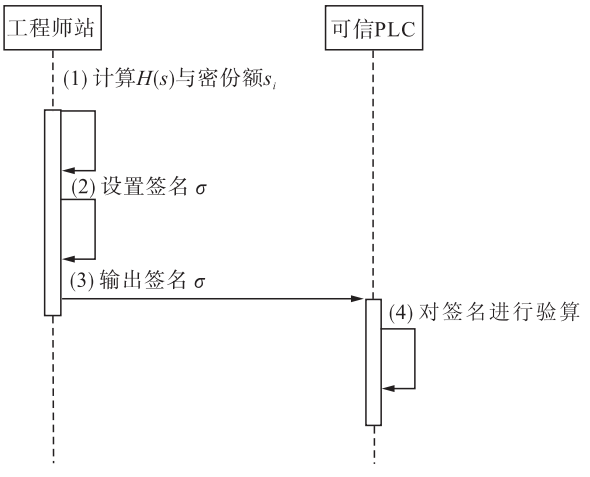

图 4　注册阶段时序图

Fig.4　Phase sequence diagram of registration stage

该阶段的 UML 时序图如图 4 所示.

3.4.3　认证阶段

在认证阶段由两个算法组成，分别是随机分量生成算法和认证算法，即 Certification-Phase = (ComApp, ComCre)，具体描述如下：

1) (C_i)←ComCre(x_i)：随机分量生成算法中假设有 $m(t\leqslant m\leqslant n)$台可信 PLC 参与认证，该算法由这 m 台参与认证的可信 PLC 执行，输入彼此公开的身份信息 x_i，输出相应的随机分量 C_i.

在此通过$\{P_j|j=1, 2, \cdots, m\}\in U$ 对这 m 台可信 PLC 进行标识，现在需要这 m 台可信 PLC 彼此之间进行验证是否属于同一组，则其中的任一参与认证的可信 PLC(公开身份为 x_i)在 GF(q)上选取随机数，并计算如下随机分量 C_i：

$$C_i=\left(f(x_i)\prod_{j=1}^{m}, j\neq i\frac{-x_j}{x_i-x_j}+r_iq\right)\bmod p \tag{17}$$

2) ComApp(C_i)：认证算法由收集到所有随机分量的可信 PLC 执行，该算法是为了确定全部 m 台参与认证的可信 PLC 是否属于同一组. 每一台参与认证的可信 PLC 通过私有信道与其他各参与认证的可信 PLC 交换随机分量 C_i. 当收到所有参与认证可信 PLC 的随机分量，即$\{C_j|j=1, 2, \cdots, m\}$后，$P_i$ 计算如下公式：

$$s'=\left(\sum_{i-1}^{m}C_i \bmod p\right)\bmod q \tag{18}$$

可信 PLC 主控通过 s'计算 $H(s')$，并将该值发送给工程师站，工程师站判断等式 $H(s')=H(s)$是否成立. 若等式成立，则表明所有参与认证的 PLC 属于同一组；反之，则可断定至少存在一台非法参与认证的 PLC，即 m 台参与认证的 PLC 终端中存在可疑的 PLC 终端参与到了认证的过程中，企图加入组内，连接到工程师站，与工程师站进行数据通信，获取工业控制系统中的重要数据.

该阶段的 UML 时序图如图 5 所示.

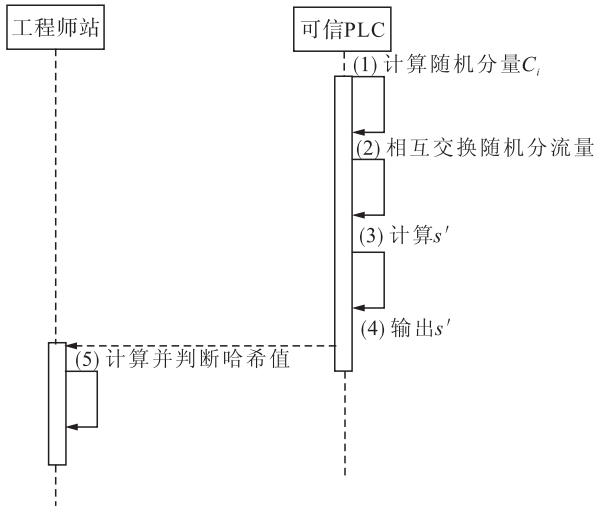

图 5　认证阶段时序图

Fig.5　Phase sequence diagram of authentication stage

4 认证模块的实现与分析

与传统的信息系统相比，工业控制系统有许多不同的特征，具体体现在操作系统、数据交换协议、实时性、故障响应、升级难度等方面，所以在实现该机制时使用可信 PLC 代替传统的 PLC，使其具有可信计算技术；设计了不仅可以支持传统用户的以太网—以太网的模式，还可以支持以太网—PCIE 模式的网络安全单元，用于数据的传输.

传统的 PLC 采用嵌入式处理器和现场可编程门阵列(FPGA)的结构，但是该结构在实际运行中无法确保执行代码的可信性，也不具备身份认证的功能. 针对上述问题，本文中的可信 PLC 采用嵌入式处理器和安全处理单元的结构，其中安全处理单元的设计机制采用 FPGA 与 TPM 安全芯片的系统架构，FPGA 作为系统的主控芯片[20-21].

由于传统以太网具有数据传输速率较低，延迟时间较长等局限性，本文在 PLC 与可信认证模块进行数据通信时是采用数据传输速率高，延迟时间短的 PCIE 协议传输替代了传统的网络接口的数据传输，PLC 与安全单元通过 PCIE 进行数据交互，确保数据在 PLC 与安全单元间传输地安全稳定性.

4.1 认证模块的实现

4.1.1 基于安全处理单元的可信 PLC 控制器

安全处理单元以可信计算技术为基础，采用可信芯片作为信任根，在安全可编程嵌入式电子设备运行阶段，安全处理单元可以实现本文机制中的接受并验证工程师站发送的签名，产生随机分量并进行组内认证等相关步骤.

该单元的安全功能除了身份认证之外，还包括系统的执行控制、虚拟化隔离、加密/解密、访问控制等关键技术，同时身份认证与密钥协商过程不干扰工业应用的执行过程. 可信 PLC 通过加密和身份认证技术，确保下装的用户控制运算代码的有效性和正确性，可信 PLC 安全防护架构如图 6 所示.

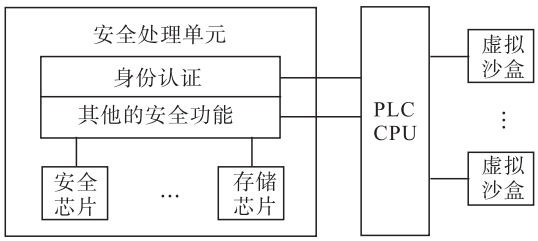

图 6 可信 PLC 安全防护架构

Fig.6 Trusted PLC safety protection architecture

4.1.2 基于 PCIE 协议的网络安全单元

国内大部分的认证产品功能单一、抗干扰性较差，严重影响系统的数据传输. 目前市场上的以太网协议转换网关或适配器大多功能单一、价格昂贵，无法适应当前低成本、高性能的产品需求. 本文中设计的网络安全单元的物理层通信接口不仅可以支持传统用户的以太网—以太网的模式，还可以支持以太网—PCIE 模式. 针对基于 PCIE 协议的传输方式，需要编写专用于 PCIE 协议的底层驱动软件，并综合数据转发、过滤等功能，上层应用软件只需将网络数据写入相关数据区，就可实现网络数据在 PCIE 中的自动发送和接收，降低通信接口改变对上层应用的影响.

该单元的数字系统由 CPU、存储资源、加解密芯片阵列和时钟等电路组成，用于运行操作系统和安全应用，并确保网络安全单元的系统性能要求，其操作系统采用 LINUX 系统. 网络安全单元的系统核心安全应用是协同可信 PLC 完成接受并验证工程师站发送的签名，产生随机分量并进行组内认证等相关步骤. 该单元的系统设备模型如图 7 所示.

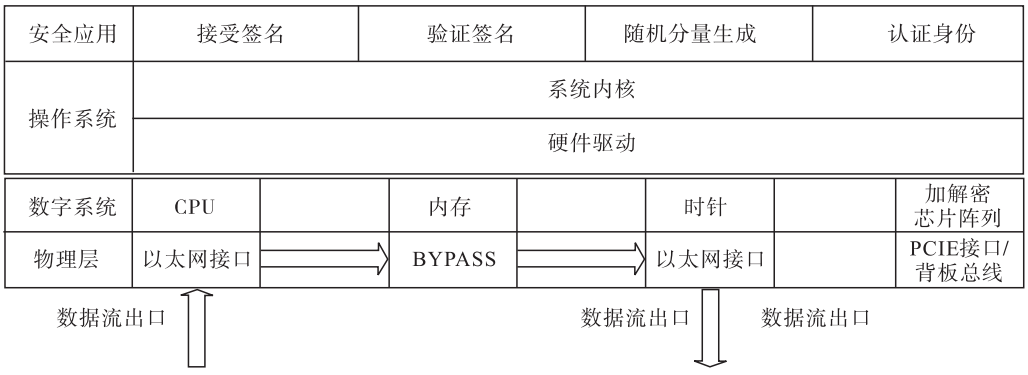

图 7 网络安全单元结构图

Fig.7 Structure diagram of network security unit

该网络安全单元数据传输时支持以太网—以太网的传输模式. 目前工业控制中进行数据传输时，主要使用工业以太网，当以太网用于工业控制时，体现在应用层的是实时通信、用于系统组态的对象以及工程模型的应用协议. 同时在该单元增加 PCIE 接口，使其支持以太网—PCIE 的传输模式，这种传输方式可以应用于任何支持 PCIE 协议的 PLC 中，数据通过背板传输，无需外部网络传输线或网络设备，确保网络数据不会外泄，最大程度上保证了未加密数据的安全性，所以在数据传输方面该网络安全单元满足大部分工业控制系统.

4.2　认证模块的分析

4.2.1　系统部署对比分析

本文改进后的机制使用了无证书签名机制，相比于传统的 PKI 认证机制，本文中的认证机制不再需要生成和管理公钥证书. 在使用改进后算法的部署图中，系统不再需要 CA/RA 服务器、LDAP 目录服务器、安全管控平台服务器和安全管控平台，也不再需要为工程师站和安全管控平台安装安全 U 盾，只需要密钥生成服务器生成部分的私钥，可以很直观地看到整个系统的部署图更加简洁，认证过程更加方便快捷，整个系统改进前后的部署图如下图所示.

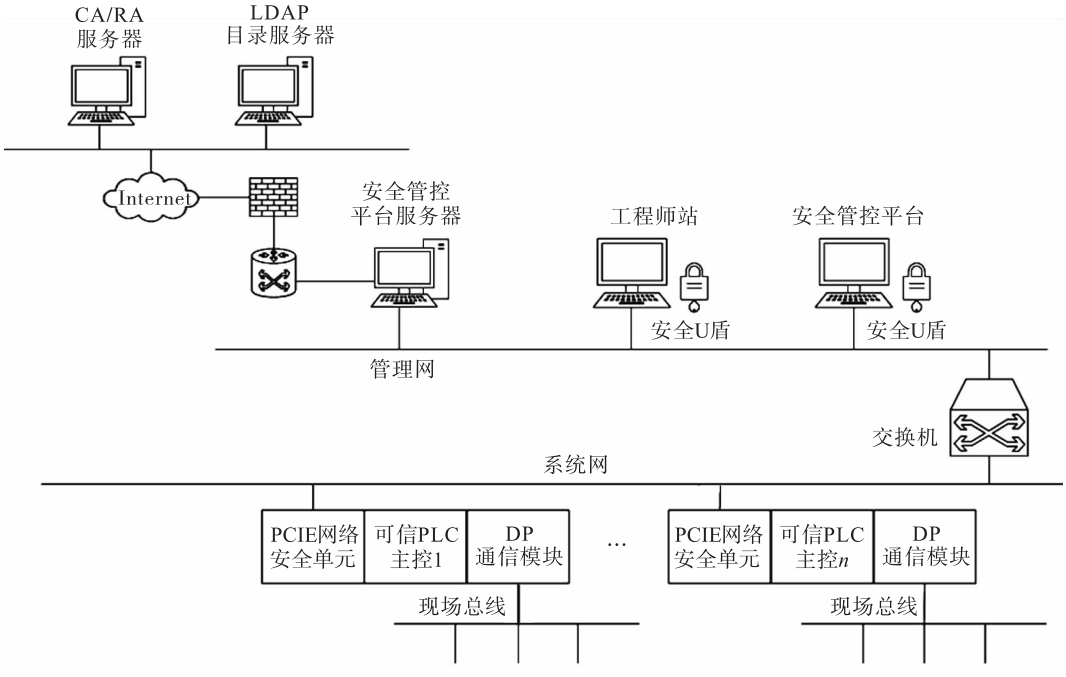

图 8　改进前的系统部署图

Fig.8　System deployment diagram before improvement

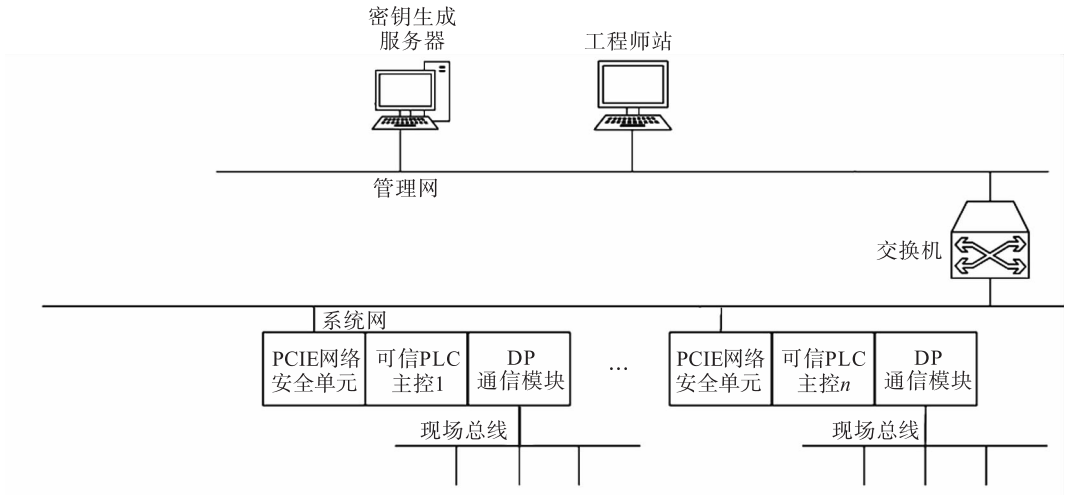

图 9　改进后的系统部署图

Fig.9　System deployment diagram after improvement

4.2.2　实用性与安全性分析

虽然有学者提出了一些解决办法，但基本都未能用于实际工控系统中，其主要原因在于：第一，许多设备供应商不支持这些改进协议；第二，对已实际部署的工控软硬件设施进行改造升级困难较大. 基于上述两个问题的存在，在实现该机制时，使用可信 PLC 代替传统的 PLC，使其具有可信计算技术，可信 PLC 采用嵌入式处理器和安全处理单元的结构；设计了不仅可以支持传统用户的以太网—以太网的模式，还可以支持以太网—PCIE 模式的网络安全单元. 可信 PLC 与安全单元通过以太网—以太网和以太网—PCIE 两种模式进行数据交互，满足大部分工业控制系统数据传输需求的同时也确保了数据在可信 PLC

与安全单元间传输地安全稳定性.

在传统的认证机制中，工程师站一次只能与一台 PLC 终端进行身份认证. 在本文的机制中，认证阶段利用了 Miao 等人提出的组认证方案，将密钥管理功能分散到 t 个或以上可信 PLC 中，用于 $m(m \leqslant n)$ 个或以上的组内可信 PLC 认证，解决密钥托管问题的同时实现了工业测控系统中多台 PLC 的群组认证，更加适用于拥有多个控制终端的工业测控系统.

由于本文中的机制使用了 Miao 等人提出的组认证方案，该方案可以同时抵御 $t-1$ 个内部攻击者的合谋攻击和 $m-1$ 个外部攻击者的合谋攻击. 将该方案进行改进应用到工业系统中后，本文中的机制同样具有 Miao 等人提出方案的优越性，在实际的工业控制系统中，本文中的机制可以同时预防 $t-1$ 台组内可信 PLC 遭到入侵以及抵御 $m-1$ 台组外的 PLC 的合谋攻击. 本文中的机制在减少计算成本的同时也增加了计算的复杂性，确保了认证过程中数据的机密性和完整性.

5 结论

本文基于无证书签名机制和门限秘密共享方案设计了一种面向工控终端的组认证机制. 本文中的机制将密钥进行了拆分，可对多台可信 PLC 同时进行认证. 本文机制中的每台可信 PLC 利用自己的身份标识生成自己的公钥和全部的私钥，不再需要公钥证书的存在，极大地降低了公钥证书管理和维护的复杂性. 本文中的机制为工业控制系统添加认证模块的同时减少了认证模块的计算量和通信开销，确保了数据传输地安全稳定性，更加适合于终端计算和存储能力有限工控网络.

在实现该机制时，使用可信 PLC 代替传统的 PLC，可信 PLC 采用嵌入式处理器和安全处理单元的结构，使其具有可信计算技术；考虑到数据传输的机密性与保密性，设计了可以支持传统用户的以太网—以太网的模式和以太网—PCIE 模式的网络安全单元. 可信 PLC 与安全单元通过以上两种模式进行数据交互，满足大部分工业控制系统数据传输需求的同时也确保了数据在可信 PLC 与安全单元间传输地安全稳定性.

本文中的机制在对工控终端进行认证时尚且停留在群组认证层面，并未对单一认证进行研究，这在一定程度上影响到了认证机制的完善性. 当使用群组认证机制检测出有终端遭到入侵时还需要有单一认证进行逐一的排查，未来会在单一认证机制上展开工作，提出更完善，更适合工控系统现场的认证机制，提高整个工业控制系统的认证能力，使工业控制系统的通信更加稳定安全.

参考文献

[1] 汪伟. 工业控制信息安全数据采集系统的设计与实现[D]. 武汉：华中科技大学，2014.
Wang W. Design and implementation of industrial control information security data acquisition system[D]. Wuhan: Huazhong University of Science and Technology, 2014.

[2] 马李翠. 智能电网的安全关键技术研究[D]. 北京：北京交通大学，2017.
Ma L C. Research on key safety technologies of smart grid [D]. Beijing: Beijing JiaotongUniversity, 2017.

[3] Khan R, Maynard P, Mclaughl-in K, et al. Threat analysis of black energy malware for synchrophasor based real-time control and monitoring in smart grid[C]//4 th International Symposium for ICS&SCADA Cyber Security Research. Piscataway, NJ, USA: IEEE, 2016: 53 - 63.

[4] Gjendemsjo M. Creating a weapon of mass disruption: Attacking programmable logic controllers[D]. Norway: Norwegian University of Science and Technology, 2013.

[5] 赵爽，马陟. 核电工控系统信息安全的密码应用研究[J]. 电脑知识与技术，2018(4)：35 - 36.
Zhao S, Ma Z. Research on password application of information security of nuclear electrical control system[J]. Computer Knowledgeand Technology, 2018(4): 35 - 36.

[6] Taylor C R, Shue C A, Paul N R. A deployable SCADA authentication technique for modern power grids[C]//Proceedings of the 2014 Energy Conference. Piscataway, NJ, USA: IEEE, 2014: 696 - 702.

[7] 张建川. 分布式认证技术研究[D]. 成都：电子科技大学，2011.
Zhang J C. Research on distributed authentication technology[D]. Chengdu: University of Electronic Science and Technology, 2011.

[8] 邵诚，钟梁高. 一种基于可信计算的工业控制系统信息安全解决方案[J]. 信息与控制，2015，44(05)：628 - 633，640.
Shao C, Zhong L G. An information security solution for industrial control system based on trusted computing [J]. Information and Control, 2015, 44(5): 628 - 633, 640.

[9] Hayes G, El-khatib K. Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol [C]// International Conference on Communications& Information Technology. Piscataway, NJ, USA: IEEE, 2013: 179 - 184.

[10] Morris T, Vaughn R, Dandass Y, et al. A retrofit network intrusion detection system for modbus RTU and ASCII industrial control system [C]//Hawaii International Conference on System Sciences. Piscataway, NJ, USA: IEEE, 2012: 2338 - 2345.

[11] TrustedComputing Group, Incorporated. TCG Trusted Network Connect IF-MAP Metadata for ICS Security[R]. Specification Version 1.0, 2014.

[12] 杨静. SCADA 系统的 Modbus/TCP 协议安全研究[D]. 北京：北京工业大学，2016.
Yang J. Research on Modbus/TCP protocol security of SCADA system [D]. Beijing University of Technology, 2016.

[13] 王勇. 基于可信计算 PLC 的身份认证与终端度量技术的研究[D]. 沈阳：沈阳理工大学，2018.
Wang Y. Research on identity authentication and terminal measurement technology based on trusted computing PLC [D]. Shenyang: Shenyang Ligong University, 2018.

[14] Abdallah A, Salleh M. Secret sharing scheme security and performance analysis[C]//2015 International Conference on Computing, Control,

Networking, Electronics and Embedded Systems Engineering(ICCNEEE). Piscataway, NJ, USA: IEEE, 2016: 83 - 93.
[15] Miao F Y, Xiong Y, Wang X F. Randomized component and its application to (t, m, n)-group oriented secret sharing[J]. IEEE Transaction-son Information Forensics and Security, 2015, 10(5): 889 - 899.
[16] 王鑫龙. 云存储下数据完整性审计技术研究与设计[D]. 合肥: 国防科学技术大学, 2016.
Wang X L. Research and design of data integrity audit technology under cloud storage [D]. Hefei: National University of Defense Technology, 2016.
[17] Sarkar P, Niandi S, Chowdhury U. Publicly verifiable secret sharing scheme in hierarchical settings using CLSC over IBC[D]. India: Indian Institute of Technology, 2013.
[18] 刘德国. 浅谈中国安全芯片技术研发的要素——以联想"恒智"为例[J]. 中国科技信息, 2014(6): 130 - 131.
Liu D G. Talking about the elements of R&D of China's security chip technology - taking Lenovo "Hengzhi" as an example [J]. China Science and Technology Information, 2014(6): 130 - 131.
[19] 李佳楠. 高速 I/O 协议数据链路层的设计与实现[D]. 西安: 西安电子科技大学, 2015.
Li J N. Design and implementation of data link layer of high speed I/O protocol [D]. Xi'an: Xidian University of Electronic Technology, 2015.
[20] 乔全胜, 邢双云, 尚文利, 等. 可信 PLC 的设计与实现[J]. 自动化仪表, 2016, 37(12): 76 - 78.
Qiao Q S, Xing S Y, Shang W L, et al. Design and Implementation of Trusted PLC[J]. Automated Instrument, 2016, 37(12): 76 - 78.
[21] 王勇, 尚文利, 赵剑明, 等. 基于 TPM 的嵌入式可信计算平台设计[J]. 计算机工程与应用, 2018, 54(13): 105 - 110.
Wang Y, Shang W L, Zhao J M, et al. Design of embedded trusted computing platform based onTPM[J]. Computer Engineering and Applications, 2018, 54(13): 105 - 110.

作者简介

尚文利(1974 -), 男, 博士, 研究员, 博士生导师. 研究领域为计算智能与机器学习, 工业信息安全.
杨路瑶(1993 -), 女, 硕士. 研究领域为工业控制系统身份认证机制.
陈春雨(1992 -), 男, 硕士, 助理研究员. 研究领域为信息安全.

(上接第 343 页)

[7] Alur R, Černý P, Zdancewic S. Preserving Secrecy Under Refinement[M]//Lecture Notes in Computer Science: vol. 4052. Berlin, Germany: Springer-Verlag, 2006: 107 - 118.
[8] Mazaré L. Using unification for opacity properties[R]//Saint Martin d'Hères, France: Verimag, Bâtiment IMAG, Université Grenoble Alpes, 2004.
[9] Bryans J, Koutny M, Ryan P. Modelling opacity using petri nets[M]//North Holland, Holland: Elsevier, 2005: 101 - 105.
[10] Bryans J, Koutny M, Mazare L, et al. Opacity generalised to transition systems[J]. International Journal of Information Security, 2008, 7(6): 421 - 435.
[11] Saboori A. Verification and enforcement of state-based notions of opacity in discrete event systems[D]. Champaign, Illinois, USA: University of Illinois Urbana Champaign, 2010.
[12] Saboori A, Hadjicostis C. Notions of security and opacity in discrete event systems[C]//46th IEEE Conference on Decision and Control. Piscataway, NJ, USA: IEEE, 2007: 5056 - 5061.
[13] Dubreil J. Monitoring and supervisory control for opacity properties[M]. Rennes, Brittany, France: Université Rennes, 2010: 89 - 96.
[14] Dubreil J, Darondeau P, Marchand H. Supervisory control for opacity[J]. IEEE Transactions on Automatic Control, 2010, 55(5): 1089 - 1100.
[15] Saboori A, Hadjicostis C. Opacity-enforcing supervisory strategies for secure discrete event systems[C]//IEEE Conference on Decision and Control. Piscataway, NJ, USA: IEEE, 2008: 889 - 894.
[16] Saboori A, Hadjicostis C. Opacity verification in stochastic discrete event systems[C]//49th IEEE Conference on Decision and Control. Piscataway, NJ, USA: IEEE: 2010: 6759 - 6764.
[17] Harel D. Statecharts: A visual formalism for complex systems[J]. Science of Computer Programming, 1987, 8(3): 231 - 274.
[18] Idghamishi A, Zad S. Fault diagnosis in hierarchical discrete event systems[C]//IEEE Conference on Decision and Control. Piscataway, NJ, USA: IEEE, 2005: 63 - 69.
[19] Brave Y, Heymann M. Control of discrete event systems modeled as hierarchical state machine[J]. IEEE Transactions on Automatic Control, 1993, 38(12): 1803 - 1819.
[20] Idghamishi A. Fault diagnosis in hierarchical discrete-event systems[D]. Montreal, QC, Canada: Concordia University, 2004.

作者简介

刘富春(1971 -), 男, 博士, 教授, 博士生导师. 研究领域为离散事件系统控制理论, 计算机控制.
严　飞(1993 -), 男, 硕士生. 研究领域为离散事件系统控制理论, 计算机控制.
赵　锐(1976 -), 女, 博士, 讲师. 研究领域为离散事件系统控制理论, 计算机控制.