文章编号:1005-0523(2019)06-0119-06

基于签密的数控机床远程操控安全交互协议

涂晓斌[1],艾美珍[1,2],易传佳[1,2],左黎明[1,2]

(华东交通大学 1.理学院; 2.系统工程与密码学研究所,江西 南昌 330013)

摘要:针对目前数控机床远程操控信息传输所存在的安全交互问题,设计了一种基于签密的数控机床远程操控安全交互协议。通过在客户端与数控机床间嵌入签密算法,实现对信息来源的可验证,防止信息泄露,确保信息的安全传输。实验仿真证实,协议具有较高的可行性。

关键词:数控机床;远程操控;签密方案;安全协议

中图分类号:TG659 文献标志码:A

DOI:10.16749/j.cnki.jecjtu.2019.06.018

数控机床是指根据事先编写的程序控制系统,通过输入指令代码自动加工零件的自动化机床。随着工业4.0的推进,数控机床已经逐渐取代了传统机床,成为国家综合实力的重要衡量标志[1]。工控系统作为国家基础设施的重要组成部分,工控系统的安全问题不仅影响着国家基础设施的安全,而且关系着广大人民群众的生命财产安全[2],如2010年伊朗的震网事件导致布什尔核电站1/5的离心机报废[3],2015年的BLACKENERGY(黑暗力量)攻击导致乌克兰持续3 h的大面积停电事故[4]。数控机床作为工控系统的应用者之一,工控系统的发展在带来便利的同时也为数控机床带来了安全问题[5],数据传输[6]的安全问题是远程操控数控机床面临的主要问题之一[7-8]。2017年,张兴宇等[9]提出基于数控机床远程监控技术的安全传输系统,实现了对传输数据的加解密,且通过实验验证了该系统的安全性。2015年,高小娟等[10]提出利用短报文通信技术和3G通信技术实现远程数据传输,并且通过建立数据中转服务器实现点对点远程数据传输。2018年,梁耀等[11]研究了工控系统中数据加密传输的可行性,设计了一种加密传输的可行性评估模型,并且提出一种算法求解数据加密长度的可行域。针对当前所提出的远程数据安全传输中身份认证与加解密分开执行,使得传输效率低的问题,本文提出了一种基于签密的数控机床远程操控安全交互协议,利用签密算法对传输过程的数据进行签密,同时实现对消息来源的身份认证和对数据的加解密,保证数控机床的数据安全。

1 预备知识

1.1 签密方案的定义

为了解决实际需求中,传递的信息能同时达到认证功能和机密性,1997年,Zheng[12]提出了签密概念,在单一逻辑中同时实现数字签名和公钥加密的全部功能,且其效率远高于传统的先签名再加密方式。签密方案各算法的具体定义描述如图1所示。

收稿日期:2019-03-19

基金项目:国家自然科学基金项目(11761033);江西省教育厅科技项目(GJJ180323,GJJ170386);江西省学位与研究生教育教学改革研究项目(JXYJG-2018-095)

作者简介:涂晓斌(1967—),男,教授,主要研究方向为工程制图。

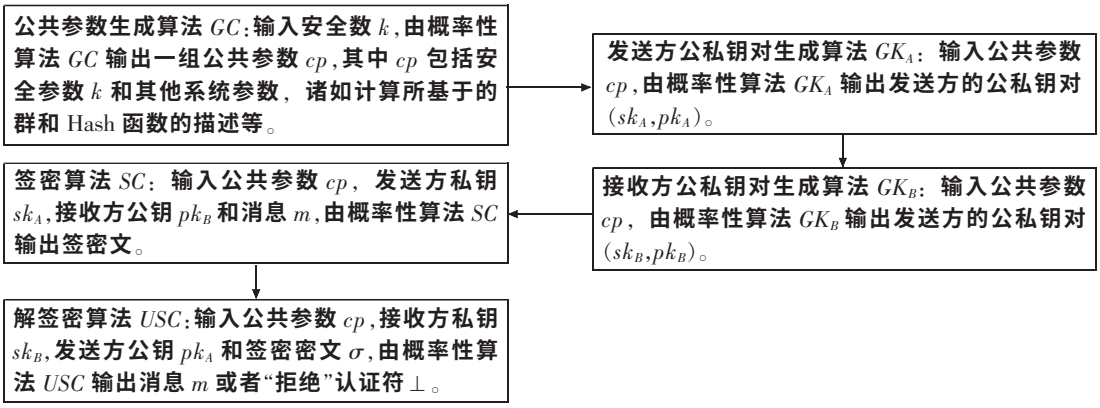

图 1 签密方案定义描述

Fig.1 Definition description of signcryption scheme

1.2 离散对数问题

设 p，q 是两个大素数，且满足 $q \mid (p-1)$，$g \in Z_p^*$ 是 q 阶元素，则 Z_p^* 中的下列问题为难解的困难问题：给定元素 $\beta \in Z_p^*$，找到整数 $\alpha \in Z_p^*$，使得 $\beta=g^{\alpha}(\mathrm{mod}\ p)$。

2 远程操控数控机床的工作原理

远程操控数控机床的主要参与者包括客户端和数控机床，其中客户端作为指令的发布者、数控机床作为指令的执行者。如图 2 所示，数控机床远程操作的基础工作原理为，客户端根据产品加工要求给出相应的操控指令，并发送给数控机床，数控机床接收到指令后，其数控装置对接收到的指令进行一系列的编译、运算、逻辑等处理后，将指令转化为数控机床可执行的消息指令，数控机床中的其他模块接收到来自数控装置的指令，各模块按照指令消息严格执行相关动作，其中伺服驱动模块主要是接受指令驱动机床移动部件，如切割位置、切割刀具等，测量反馈模块主要是反馈机床实际位移到数控装置，以便数控装置调整指令，辅助控制模块主要是接受指令控制数控机床的开关量动作，如液压、气动等的开关量，使得数控机床高效有序的进行产品加工。

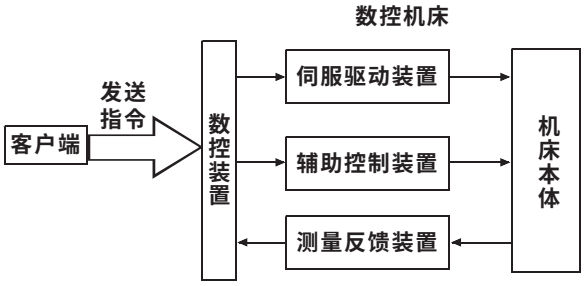

图 2 数控机床结构图

Fig.2 Structure diagram of CNC machine tool

3 文献[12]的方案回顾

1）系统参数：p，q 是两个大素数，且满足 $q \mid (p-1)$，$g \in Z_p^*$ 是 q 阶元素，$x_a \in Z_q^*$ 是发送者的私钥，$y_a \in g^{xa}(\mathrm{mod}\ p)$ 是发送者的公钥，$x_b \in Z_q^*$ 是接收者的私钥，$y_b=g^{xb}(\mathrm{mod}\ p)$ 是接收者的公钥，H 是抗碰撞的 Hash 函数，(E,D) 是安全的对称加解密对。

2）签密过程：发送者对消息进行以下签密过程：

① 发送者随机选取 $k \in Z_q^*$，计算 $K=H(y_b^k \bmod p)$；

② 计算 $c=E_k(m)$；

③ 令 $r=H(H(m),g^k \bmod p)$，计算 $R=g^r \bmod p$；

④ 计算 $s=k(r+x_a)^{-1} \bmod q$，输出发送者对消息 m 的签密密文 (c,R,s)，并发送给接受者。

3）解签密过程：接收者收到发送者对消息 m 的签密密文 (c,R,s)，并进行以下解签密过程：

① 计算 $K=H((y_a R)^{sxb} \bmod p)$；

② 计算 $m=D_K(c)$；

③ 验证等式 $R=g^{H(H(m),(y_a R)^s \bmod p)} \bmod p$，若签密验证等式成立，则签密密文有效，接收者接受秘密消息和发送者的签名。

4）上述签名验证等式的正确性证明如下：

$$g^{H(H(m),(y_a R)^s \bmod p)} \bmod p$$

$$=g^{H(H(m),(g^{r+x})^s \bmod p)} \bmod p$$

$$=g^{H(H(m),g^k \bmod p)} \bmod p$$

$$=g^r \bmod p=R$$

4　基于签密的数控机床远程操控设计

远程操控数控机床主要是由计算机通过无线将指令传输到数控机床，而此过程极易被不法分子攻击，导致数据的泄露、篡改等。为保证远程操控数控机床的数据交互过程的安全性，对数据交互过程嵌入签密算法。对于本方案所构建的客户端计算机，其包括了机床信息查看模块、数据处理模块以及签密模块，而对于数控机床中的数控模块，其包括了解签密、消息处理以及数控装置的调控机床加工功能，同时数控机床中的其他模块功能不变。本方案的整体方案设计架构如图 3 所示。

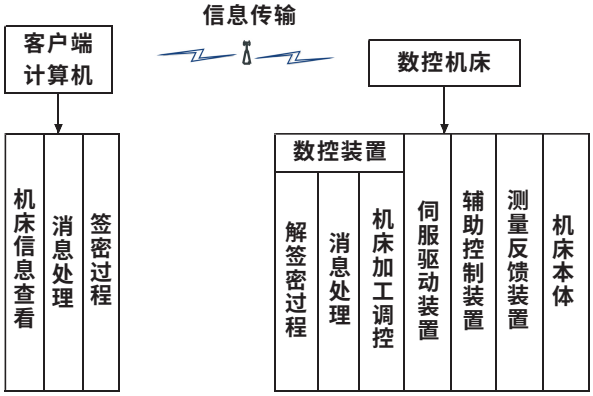

图 3　整体方案架构图

Fig.3　Overall schematic architecture

对于本文所提出的远程操控数控机床方案，其实现过程如下。计算机选择加工的数控机床，查看机床当前状态，输入相关操作指令，并对指令等数据做标准化处理，使得数据满足特定的标准格式，然后对数据消息进行签密操作，并发送至相应的数控机床。数控机床接收到消息，首先对消息进行解签密操作，验证发送者的身份，验证通过后，将得到的数据消息通过消息处理模块，使得数据被分解为具体的指令消息，传递给数控模块，数控模块将读取的消息转化为机床可执行的指令，伺服模块收到指令对产品进行切割加工，辅助控制模块收到指令对加工时温度、气压等进行控制，而测量反馈模块主要是将检测加工产品的实际加工位置值反馈到数控模块，数控模块将实际值与指令值对比，调整指令。

5　数控机床远程操控的安全协议

5.1　符号说明

为了方便协议的描述，本文对协议所涉及的符号进行了说明解释，如表 1 所示。

5.2　数据封包设计

客户端将需要发送至数控机床的指令信息采用 packet 封包消息处理机制处理后，再对其指令进行签密操作，然后对签密后的信息再次使用 packet 封包消息处理机制，再将消息发送至数控机床。其中 packet 封包消息处理方式是将不同数据块用“#”拼接，如客户端对需要发送的数控机床指令，其格式为

CID#MID#SPo int#*EPo int#LShape#CTool#CSpeed#CTemp#CPress*

5.3 安全协议实现

5.3.1 参数生成

一个可信任的权威机构执行下列操作：

1）选择两个大素数 p，q，满足 $q \mid (p-1)$，选择 $g \in Z_p^*$ 是 q 阶元素。

2）选择一个抗碰撞的 Hash 函数 H。

3）建立安全的对称加、解密对算法：(E,D)。

面向系统范围内所有用户，公开参数 (p,q,g,H,E,D)。

5.3.2 用户公私钥建立

系统范围内的所有用户，不论是消息的发送者（客户端计算机）还是接收者（数控机床），都有其相应的公私钥对，公私对的生成过程如下：

1）用户 *ID* 随机选择随机数 $x_{ID} \in Z_p^*$ 作为私钥，秘密保存。

2）用户 *ID* 根据选取的私钥，计算 $y_{ID}=g^{xID} \pmod p$ 作为其公钥，并公开。

表 1 符号说明

Tab.1 Symbolic explanation

符号	说明
CID	计算机唯一标识
MID	数控机床唯一标识
SPoint	切割起点
EPoint	切割终点
LShape	切割线形状
CTool	切割刀具
CSpeed	切割速度
CTemp	切割温度
CPress	切割气压

5.3.3 签密过程

1）数据处理。唯一标识码为 *CID* 的计算机根据产品加工要求选择相应唯一标识码为 *MID* 的数控机床，输入相应的加工要求，如切割起点 *SPoint*、切割终点 *SPoint*、切割线形状 *LShape*、切割刀具 *CTool*、切割速度 *CSpeed*、切割温度 *CTemp* 以及切割气压 *CPress* 等，并按照所设计的 packet 封包格式将数据处理为 *CID#MID#SPoint#EPoint#LShape#CTool#CSpeed#CTemp#CPress*。

2）签密算法。计算机 *CID* 对经过 packet 封包处理机制的数据消息 *m=CID#MID#SPoint#EPoint#LShape#CTool#CSpeed#CTemp#CPress* 进行签密，其过程如下：

① 计算机 *CID* 随机选择 $k \in Z_q^*$，计算 $K=H(y_{MID}^{\ k} \bmod p)$；

② 计算 $c=E_K(m)$；

③ 令 $r=H(H(m),g^k \bmod p)$，计算 $R=g^r \bmod p$；

④ 计算 $s=k(r+x_{CID})^{-1} \bmod q$。

计算机 *CID* 将签密密文以 (c,R,s) 形式发送给数控机床 *MID*。

5.3.4 解签密过程

数控机床 *MID* 对收到签密密文 (c,R,s) 进行解签密，其过程如下：

① 数控机床 *MID* 首先计算 $K=H((y_{CID}\ R)^{sxMID} \bmod p)$；

② 解密消息：$m=D_k(c)$；

③ 签名验证：$R=g^{H(H(m),(y_{CID}R)^s \bmod p)} \bmod p$，若等式不成立，则放弃继续操作，否则接收消息。

5.3.5 消息处理及机床加工调控

数控机床对解签密后的消息进行进一步处理，将消息处理为数控机床可读的指令，并根据指令调控机床的其他模块，进行产品加工。

5.4 安全性分析

本文所提出方案的安全性基于 1.2 节中困难问题的难解性，以此保证协议的安全性。

5.4.1 不可伪造性

假设攻击者根据发送者的签密过程伪造上述协议中的签名密文 (c',R',s')，若要使得签名密文 (c',R',s') 成立，则签名密文 $(c',R',s') \bmod p$ 应满足上述解签密过程中的签名验证等式 $R'=g^{H(H(m'),(y_{CID}R)^{s'} \bmod p)} \bmod p$。

即满足 $g^{k'}=(y_{SID}R')^{s'} \bmod p=g^{(r'+x_{SID})s'}$。由此可知，要使签名密文有效，需要 s' 满足等式 $s'=k'(r'+x_{SID})^{-1} \bmod q$，但是由于 x_{SID} 是保密的，又因为 $y_{SID}=g^{x_{SID}} \bmod p$，而 y_{SID} 与 x_{SID} 是嵌套在离散对数问题中；因此计算 x_{SID} 就是解离散对数问题。综上所述，攻击者所伪造的签名密文 (c',R',s') 不满足上述协议中的签名密文。

5.4.2　机密性

假设攻击者截获到计算机 *CID* 发送给数控机床 *MID* 的签名密文 (c,R,s)，对于密文 (c,R,s)，若攻击者要求解出消息 m，需要攻击者对密文解密，得到消息 $m=D_K(c)$，而对于攻击者的解密过程，需要得到 $K=H((y_aR)^{sxMID} \bmod p)$，又由于 K 是关于 x_{MID} 的等式，因此计算 K，需要先求解 x_{MID}，又因为 $y_{MID}=g^{xMID} \bmod p$ 是一个离散对数问题，因此攻击者不能求解出 x_{MID}，因此攻击者不能通过签名密文 (c,R,s) 求解出消息 m。

5.5　关键技术的实验仿真

在 Windows7 系统的 Visual Studio 2012 软件开发平台下，利用平台中的控制台应用程序结合 BouncyCastle 库和本文所设计安全协议，模拟数控机床的远程操控实现数控机床加工产品，其核心代码实现如下：

```
/********* 客户端的签密过程 *********/
string m=CID+"#"+MID+"#"+SPoint+"#"+EPoint+"#"+LShape+"#"+
    CTool+"#"+CSpeed+"#"+CTemp+"#"+CPress; //消息处理
string c = AES.Encode(m, K);//对消息加密 c=EK(m)
BigInteger r = new BigInteger(myhash.TanGetDigestByteArray(t1));//计算 r=h(h(m),g^k)
ECPoint R = eccparam.ecc_point_g.Multiply(r);//计算 R=g^r
BigInteger s = k.Multiply(l.Divide(r.Add(x1))).Mod(q);//计算 s=k(r+x1)^-1
/******* 数控机床的解签密过程 *********/
//计算对称密钥 K1=h((y1R)^sx2)modp
string K1 = myhash.TanGetDigest(y1.Add(R).Multiply(s.Multiply(x2)).ToString());
string m1 = AES.Decode(c, K1); //计算 m1=DK1(c)
/************** 签密验证 **************/
BigInteger temp = new BigInteger(myhash.TanGetDigestByteArray(t2)); //计算 h(h(m1),(y1R)^s)
ECPoint R1 = eccparam.ecc_point_g.Multiply(temp); //计算 R1=g^h(h(m1),(y1R)^s)
if (R.Equals(R1)){
    Console.Out.WriteLine("等式左右相等，签名验证成功");
}
```

6　结论

本文利用签密方案为数控机床远程操控设计了一种基于 packet 封包消息处理机制的信息安全交互协议，强化了客户端与数控机床之间信息交互的安全性，能有效的避免传输的信息内容被第三方获取、篡改，以及可以抵抗黑客的大部分攻击。使用具有前向安全性的可公开验证的签密方案提高了协议的安全性以及计算效率，并通过实验仿真，证明数控机床远程操控的可信性和安全性。

参考文献：

[1] 唐克岩. 我国数控机床产业发展现状与展望[J]. 机床与液压，2012，40(5)：145-147.

[2] 陶耀东，李宁，曾广圣. 工业控制系统安全综述[J]. 计算机工程与应用，2016，52(13)：8-18.

[3] 张家年. 国家安全保障视角下安全情报与战略抗逆力融合研究——伊朗核设施遭“震网”病毒攻击事件的启示[J]. 情报杂志，2018，37(2)：8-14.

[4] 李保杰,刘岩,李洪杰,等. 从乌克兰停电事故看电力信息系统安全问题[J]. 中国电力,2017,50(5):71-77.
[5] 李丽丽,史建锋,赵波,等. 数控机床安全性发展现状[J]. 机床与液压,2014,42(17):176-178.
[6] 谢昕,汪加楠,姜楠,等. WSN 中改进的基于压缩感知的分簇数据采集算法[J]. 华东交通大学学报,2018,35(2):113-119.
[7] 田齐. 基于网络的数控机床远程监控与管理系统设计与实现[J]. 机床与液压,2015,43(22):167-171.
[8] 刘杰,汪京培,李丹,等. 数控机床自动化网络信息安全综合防护方案[J]. 组合机床与自动化加工技术,2016(3):82-85.
[9] 张兴宇,韩秋实,彭宝营. 基于数控机床远程监控技术的安全传输系统开发[J]. 组合机床与自动化加工技术,2017(6):82-85.
[10] 高小娟,车明,黎贺. 异构网络制式下的 3G 点对点远程数据传输[J]. 计算机工程,2015,41(9):120-125.
[11] 梁耀,冯冬芹,徐珊珊,等. 加密传输在工控系统安全中的可行性研究[J]. 自动化学报,2018,44(3):434-442.
[12] ZHENG Y. Digital signcryption or how to achieve cost (signature & encryption)? cost (signature)+ cost (encryption)[C]//Annual International Cryptology Conference. Springer,Berlin,Heidelberg,1997: 165-179.
[13] 戚明平,陈建华,何德彪. 具有前向安全性的可公开验证的签密方案[J]. 计算机应用研究,2014,31(10):3093-3094.

Security Interaction Protocol for Remote Control of CNC Machine Tools Based on Signcryption

Tu Xiaobin[1], Ai Meizhen[1,2],Yi Chuanjia[1,2], Zuo Liming[1,2]

(1.School of Science; 2. Institute of Systems Engineering and Cryptography, East China Jiaotong University Nanchang 330013, China)

Abstract: Aiming at the problem of information security interaction in the transmission of remote control for CNC machine tool, a secure interaction protocol for remote control of CNC machine tool based on signcryption is designed. By embedding the signcryption algorithm between client and CNC machine tool, the verifiability of information source can be realized, which can prevent information leakage and ensure the safe transmission. The experimental simulation proves that the protocol has high feasibility.

Key words: CNC machine tool; remote control; signcryption scheme; security protocol