国密算法在工业互联网安全中的应用研究*

苏彬庭[1,2],陈明志[3],许 力[1,2],周赵斌[1,2]

(1.福建师范大学 网络与数据中心,福建 福州 350117;
2.福建省网络安全与密码技术重点实验室,福建 福州 350007;3.北卡科技有限公司,福建 福州 350000)

摘 要: 工业互联网安全是网络空间安全的重要组成部分。加强国密算法在工业互联网中的应用研究,对于提高我国网络空间安全的防护能力和实现自主化目标具有重大意义。阐述了国密算法在工业互联网的应用现状和存在的挑战,并基于国密算法设计一种轻量级的身份认证协议。分析表明,该协议两次握手可完成认证,并能够满足认证的安全性要求,具有良好的应用价值。

关键词: 国密算法;工业互联网;认证协议

中图分类号: TN918.9 **文献标识码:** A **DOI:** 10.19358/j.issn.2096-5133.2021.03.005

引用格式: 苏彬庭,陈明志,许力,等. 国密算法在工业互联网安全中的应用研究[J].信息技术与网络安全,2021,40(3):28-31.

Application research of national secret algorithm in industrial Internet security

Su Binting[1,2], Chen Mingzhi[3], Xu Li[1,2], Zhou Zhaobin[1,2]

(1.Network and Data Center, Fujian Normal University, Fuzhou 350117, China;
2.Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou 350007, China;
3.Beika Technology Co., Ltd., Fuzhou 350000, China)

Abstract: Industrial Internet security is an important part of cyberspace security. Strengthening the research on the application of national cryptographic algorithms in the industrial Internet is of great significance for improving country's cyberspace security protection capabilities and achieving autonomous controllable goals. This paper expounds the application status and challenges of the national secret algorithm in the industrial Internet, and designs a lightweight identity authentication protocol based on the national secret algorithm. Analysis shows that the protocol can support authentication within two handshakes, and meets the security requirements of authentication. Hence, the proposal has good application value.

Key words: national secret algorithm; industrial Internet; authentication protocol

0 引言

网络空间安全在我国的主权维护与安全防控中扮演着重要的角色,密码技术作为网络空间安全的“命脉”,是国家的战略资源和维护网络空间安全的根本。然而,当前部分主流密码算法(例如 DES、SHA1、RSA 等)不仅存在安全性或使用不规范的问题[1-4],同时也无法满足我国对网络空间安全自主化要求[5]。为解决这一问题,我国近几年加大国产密码算法(以下简称“国密算法”)研究工作,并取得了关键性进展。随着工业化与信息化的深度融合,工业互联网安全已经成为网络空间安全重要问题之一。工业互联网系统间的互联特性,将使其核心工业生产控制系统面临更多的安全威胁[6]。工业互联网是新一轮工业革命和产业变革的一个重点发展领域,推进国密算法的研究与应用,从根本上解决终端信息存储、认证、数据传输等问题,对于保障我国工业互联网安全和实现网络安全的自主化目标具有重大意义。本文首先阐述了国密算法在工

* 基金项目:国家自然科学基金(U1905211);企事业合作项目(DH-1565);福建省中青年教师教育科研项目(JAT200080);福建省“十四五”教育发展专项规划课题(JSZ19021)

业互联网中的应用以及面临的挑战，针对工业互联网终端的身份识别问题，设计一种轻量的安全身份认证协议，该协议具备双向认证、前向安全性、支持用户撤销、抵抗攻击等安全特性。

1 国密算法在工业互联网安全中的应用与挑战

1.1 国密算法介绍

国密算法在商用领域已经形成完整的基础型密码体系，如表 1 所示，包括 SM1、SM3、SM4、SM7、SM9 和 ZUC 等密码算法[7-10]。这些算法不仅是获得国家批准的行业密码标准，其中 SM2、SM3、SM9 和 ZUC 密码算法相继通过了 ISO/IEC 信息安全分技术委员会评审，成为国际标准。验证表明，SM2 的安全性要高于国际通用的 ECDSA 算法，SM3 的安全性与 SHA-256 相当，但高于 MD5、SHA-1、SHA-224[10-11]。

表 1 国产密码算法及其应用

名称	类型	是否公开	应用
SM1	对称密码算法	否	电子政务、电子商务
SM2	公钥密码算法	是	签名验签系统、密码机
SM3	杂凑算法	是	VPN、密码键盘
SM4	对称密码算法	是	VPN
SM7	对称密码算法	否	IC 卡
SM9	公钥密码算法	是	云端数据加密
ZUC	对称密码算法	是	图像加密

1.2 应用现状

2020 年 1 月 1 日，我国颁发了《中华人民共和国密码法》，明确规定“涉及国家安全、国计民生、社会公共利益的商用密码产品，在获得具备资格的机构检测认证合格前，不可销售或者提供”，规范了各类商用密码产品的使用和上市条件。目前，各类需要密码算法的设备、软件和系统等产品，主要采用的是国际通用的密码算法，集成国密算法相对较少。

在工业互联网安全领域中，国密算法的应用主要体现在身份认证、访问控制、账户管理、数据安全等方面，涉及通信协议、认证协议、电子签名等关键技术[10,12-16]。通常利用 SM1、SM4、SM7 和 ZUC 序列等对称密码算法加解密数据，保证数据的保密性；利用 SM2 和 SM9 等非对称密码算法产生消息签名，保证数据的不可否认性；利用 SM3 杂凑算法计算消息摘要，保证数据的完整性。各大企业也研制出国密加密芯片、服务器密码机、云服务器密码机、VPN 设备和加密硬盘等数据加密类产品，以及签名验签服务器和电子签章数据签名类产品。

1.3 存在的挑战

国产密码在工业互联网中的应用面临着诸多挑战：

(1)研究起步晚，集成国密算法的产品较少。我国在 1996 年才开始重视国产密码算法的研究，研究起步较晚。此外，商用密码检测机构偏少，影响产品的认证周期和成本，延长了产品上市时间，降低了产品的竞争力，从而降低了各企业研发的产品集成国密算法的积极性。

(2)产品多数采用双芯片结构，效率低。多数密码商用产品采用双芯片结构，如图 1 所示，待处理的数据通过主芯片向国密芯片传输，经国密芯片进行密码运算后，再回传到主芯片进行业务操作。这种结构导致产品计算和运行效率降低，同时增加数据在两个芯片传输过程的泄露风险。

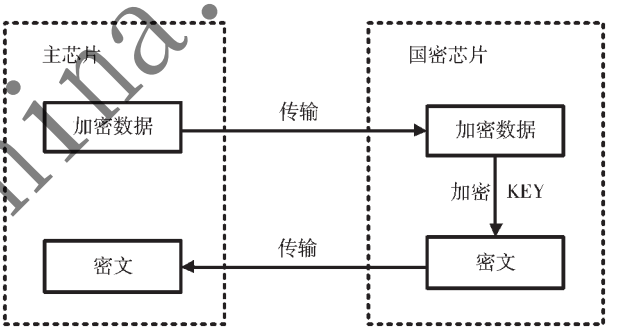

图 1 双芯片结构示意图

(3)信息系统无法支持基于国产密码算法的传输/认证协议。目前工业信息系统主要是 B/S 架构，数据在客户端和服务器之间的传输安全性主要基于国际 SSL/TLS 协议。虽然目前研究学者设计了各种基于国密算法的 SSL/TLS 协议[16-17]，市场上也存在多款支持国密算法的浏览器(例如密信)，但多数企业前期建设的信息系统无法支持，且改造难度大，导致信息无法基于国产 SSL/TLS 协议进行传输。

本文在工业互联网环境下，从物联网终端的身份鉴别问题出发，设计一种基于国密算法的高效安全身份认证协议。

2 安全身份认证协议

本文提出的安全身份认证协议只需 2 次握手即可完成双方的身份认证，认证过程使用 SM3、SM4 确保数据的完整性和保密性。如图 2 所示，在终端

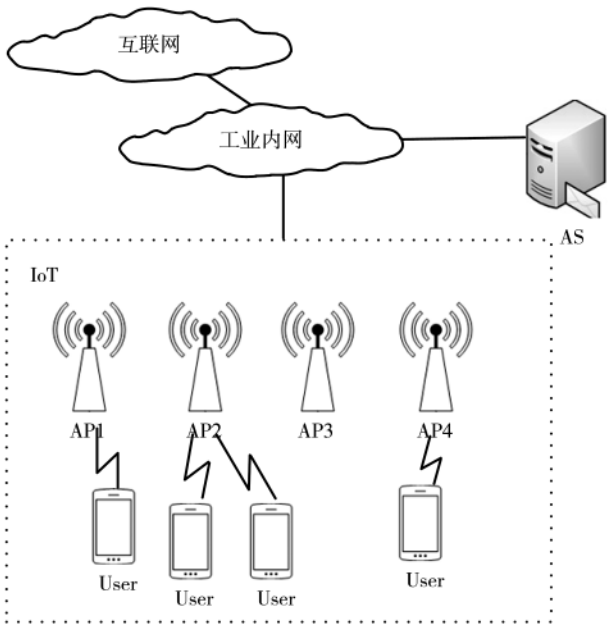

图 2 工业互联网拓扑图

加入网络前,认证服务器(Authentication Server,AS)通过安全通道向系统的接入点(Access Points,AP)和物联网终端预分发相关秘钥。

2.1 系统初始化

在系统初始化过程中,认证服务器输入安全参数 k 执行密钥生成算法,为网络终端和接入点创建秘钥对。

(1)选择一大素数 q 和 p,E/F_p 是定义在有限域 F_p 上的椭圆曲线。选择 E/F_p 上的一个阶为 q 的点 P,生成循环加法群 G;

(2)随机选择参数 $s \in Z_q^*$,计算系统公钥 $PK=s \cdot P$;

(3)杂凑算法 $SM3(m)$:使用 SM3 算法计算消息 m 的消息摘要;

(4)对称加密算法 $SM4(key,m)$:使用秘钥 key,通过 SM4 算法加密消息 m;

(5)公开系统参数 $\{q,p,E/F_p,P,G,PK\}$。

AS 根据系统参数为网络每个接入点创建公私钥对。假设 ID_{AP} 为每个接入点的唯一身份标识,AS 选择随机数 $r_{AP} \in Z_q^*$,计算 $R_{AP}=r_{AP} \cdot P$,$h_{AP}=SM3(ID_{AP}|R_{AP})$ 和 $s_{AP}=r_{AP}+s \cdot h_{AP}$,将 (s_{AP},R_{AP}) 通过安全通道发给 AP。AP 收到密钥后,计算公钥 $PK_{AP}=s_{AP} \cdot P$ 并定期广播自身信息 (ID_{AP},R_{AP})。AS 为每个终端生成 ID_u,选择随机数 $a \in Z_q^*$,将 $\{ID_u,a\}$ 通过安全通道发给终端存储,并计算终端的认证参数 $A=a \cdot P$。

2.2 认证协议

在系统的运行过程中,AS 会定期广播 User 的列表信息,包括 ID_u 和认证参数 A。当用户加入网络时,需要先通过 AP 的认证后,才允许与业务网进行通信,认证过程如图 3 所示。

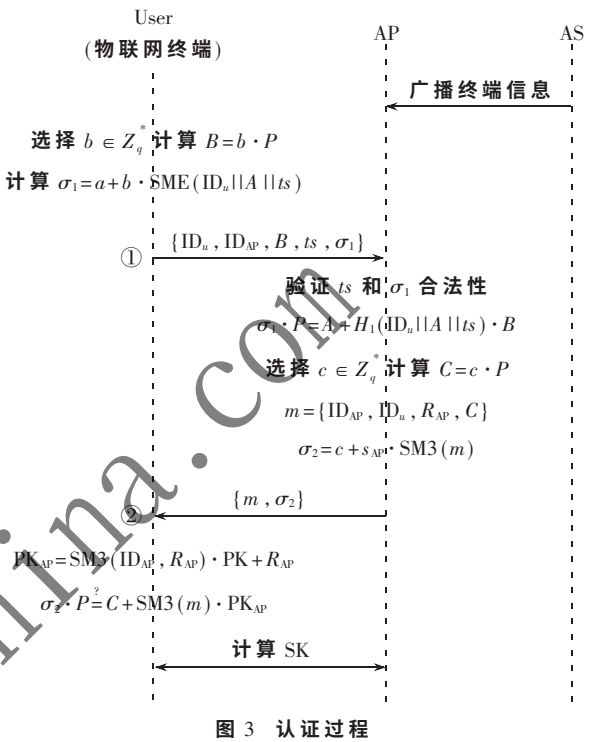

图 3 认证过程

(1)User->AP:终端加入网络时,首先选择随机数 $b \in Z_q^*$,计算 $B=b \cdot P$,并产生签名 $\sigma_1=a+b \cdot SM3(ID_u||A||ts)$。最终将消息 $\{ID_u,ID_{AP},A,ts,\sigma_1\}$ 发送给 AP 请求接入网络。

(2)AP->User:AP 收到 User 的请求后,首先根据式(1)验证签名和时间戳的合法性。如果合法,从用户列表中取出该终端的认证参数,选择随机数 $c \in Z_q^*$ 计算 $C=c \cdot P$,并产生签名 $\sigma_2=c+s_{AP} \cdot SM3(m)$,其中 $m=\{ID_{AP},ID_u,R_{AP},C\}$,将 $\{m,\sigma_2\}$ 发送给 User。

$$\sigma_1 \cdot P \stackrel{?}{=} A+H_1(ID_u||A||ts) \cdot B \quad (1)$$

$$PK_{AP}=SM3(ID_{AP},R_{AP}) \cdot PK+R_{AP} \quad (2)$$

$$\sigma_2 \cdot P \stackrel{?}{=} C+SM3(m) \cdot PK_{AP} \quad (3)$$

User 收到消息后,首先根据式(2)计算公钥 PK_{AP}。再根据式(3)验证签名 σ_2 的合法性,如果合法,则完成认证过程。AP 和 User 根据式(4)生成会话秘钥。

$$SK=b \cdot C=c \cdot B \quad (4)$$

2.3 协议安全性分析

(1)双向认证：AP 通过 User 的身份 ID 以及秘钥参数，验证 User 的身份信息；User 利用系统公开的公钥 PK 验证 AP 的合法性，认证过程实现了双向认证。

(2)前向安全性：在终端请求认证时，认证消息加入了时间戳，而且对于同个终端，AP 每次生成的认证参数都不相同。因此，即使 AP 或 User 秘钥参数泄露，也无法计算出之前使用过的会话秘钥。

(3)支持用户撤销：AS 和 AP 都维护了系统终端的 ID 列表，如果需要撤销某个终端接入权限，只要在 AS 做撤销操作，并将列表更新发送至 AP 即可。

(4)抵抗攻击：认证过程加入了时间戳，并且认证双方在每次认证中，选择了不同的随机数作为认证参数，可有效抵抗重放攻击。

3 结论

本文首先介绍了国密算法在工业互联网安全领域中的应用情况，并提出了当前存在的挑战。其次根据国密算法在工业互联网应用中存在的问题，设计一种高效安全的身份认证协议，解决物联网终端加入工业互联网时，无法基于国密算法进行身份认证的问题。分析表明，该协议满足双向认证、支持用户撤销、抵抗重放攻击等安全要求，完成认证仅需 2 次握手，认证效率高，可进一步加强工业互联网的安全建设，提高网络安全防护能力，具有良好的应用推广价值。

参考文献

[1] 张焕国，韩文报，来学嘉，等.网络空间安全综述[J].中国科学：信息科学，2016，46(2)：125-164.

[2] 李鸿培，李强.工业互联网的安全研究与实践[J].电信网技术，2016(8)：20-26.

[3] 黄健.RSA 公钥加密体制的安全性分析与改进[J].计算机与网络，2016，42(1)：70-73.

[4] 潘建生，孔苏鹏，程实.实现 DES 加密算法安全性的分析与研究[J].网络空间安全，2020，11(4)：104-107.

[5] 秦志光.密码算法的现状和发展研究[J].计算机应用，2004(2)：1-4.

[6] 骆钊，严童，谢吉华，等.SM2 加密体系在智能变电站远动通信中的应用[J].电力系统自动化，2016，40(19)：127-133.

[7] 王小云，于红波.SM3 密码杂凑算法[J].信息安全研究，2016，2(11)：983-994.

[8] 姚键.国产商用密码算法研究及性能分析[J].计算机应用与软件，2019，36(6)：327-333.

[9] XIE Y Q.China's cryptographic algorithm application[J].Journal of Information Security Research，2016(2)：969-971.

[10] 柳彩云，陈雪鸿，杨帅锋.国产密码算法与工业互联网平台的结合势在必行[J].中国信息安全，2019(4)：86-89.

[11] 孙荣燕，蔡昌曙，周洲等.国密 SM2 数字签名算法与 ECDSA 算法对比分析研究[J].网络安全技术应用，2013(2).

[12] LIU R，ZOU Y J，CHEN X F，et al.Electronic aircraft maintenance record signature technology based on SM2 cryptographic algorithm[C].2019 IEEE 1st International Conference on Civil Aviation Safety and Information Technology(ICCASIT)，2019.

[13] 李秀滢，吉晨昊，段晓毅，等.GPU 上 SM4 算法并行实现[J].信息网络安全，2020，20(6)：36-43.

[14] 黎水林，陈广勇，柳盈，等.商用密码在政府网站中的应用研究[J].信息网络安全，2019：48-51.

[15] 苏吟雪，田海博.基于 SM2 的双方共同签名协议及其应用[J].计算机学报，2020，43(4)：701-710.

[16] 朱义杰，杨玉龙，杨义，等.一个基于国密算法的 RFID-SIM 系统安全认证协议[J].网络安全技术与应用，2019(11)：34-36.

[17] 刘迪，牟鹏，董爱强.基于国密算法安全中间件的安全功能研究与设计[J].网络安全技术与应用，2017(4)：74-78.

(收稿日期：2020-01-28)

作者简介：

苏彬庭(1990-)，男，硕士，工程师，主要研究方向：网络与信息安全、大数据与信息化。

陈明志(1975-)，男，博士，教授，主要研究方向：互联网安全通信、智能信息处理等。

许力(1970-)，男，博士，教授，主要研究方向：网络与信息安全、云计算与物联网、大数据与信息化、智能信息处理。