

电力物联终端侧安全防护密码算法研究

吴飞^{1†}, 谢毅², 何德明¹, 孔美美¹, 刘宇轩²

(1. 国网福建省电力有限公司, 福建 福州 350001; 2. 国网福建省电力有限公司宁德供电公司, 福建 宁德 352000)

摘 要:电力物联终端侧需要能够应对各种类型的安全攻击,如侧信道攻击、重放攻击、中间人攻击等。密码算法需要具备足够的抗攻击能力,能够抵御已知的攻击方法,并能及时适应新型的安全威胁。为此,提出了一种电力物联终端侧安全防护密码算法。建立并分析电力物联终端结构,采用 SM9 密码算法对电力物联终端侧接口数据做加密处理,并设计算法流程;为优化加密效果,利用密文和密文的映射生成乱序密文;通过用户的公开密钥和用户隐私安全标识与公开密钥构成的接口数据包,设计面向用户隐私信息的安全防护密码算法。实验结果显示:研究提出的电力物联终端侧密码算法应用下,接口数据和用户隐私数据的丢失率更低。

关键词:电力;物联终端侧;安全防护;SM9 密码算法

中图分类号:TP39

文献标识码:A

Research on Security Protection Password Algorithm for Power IoT Terminal Side

WU Fei^{1†}, XIE Yi², HE Deming¹, KONG Meimei¹, LIU Yuxuan²

(1. State Grid Fujian Electric Power Co., Ltd., Fuzhou, Fujian 350001, China

2. State Grid Fujian Electric power Co., Ltd., Ningde Power Supply Public, Ningde, Fujian 352000, China)

Abstract: The power IoT terminal side needs to be able to cope with various types of security attacks, such as side channel attacks, replay attacks, and man in the middle attacks. Cryptography algorithms need to have sufficient anti attack capabilities, be able to resist known attack methods, and be able to adapt to new security threats in a timely manner. To this end, a security protection password algorithm for the power IoT terminal side is proposed. Establish and analyze the structure of the power IoT terminal, use the SM9 encryption algorithm to encrypt the interface data of the power IoT terminal, and design the algorithm process. To optimize the encryption effect, use the mapping of ciphertext and ciphertext to generate unordered ciphertext. Design a security protection password algorithm for user privacy information through an interface data packet composed of the user's public key, user privacy security identifier, and public key. The experimental results show that under the application of the proposed power IoT terminal side password algorithm, the loss rate of interface data and user privacy data is lower.

Key words: electricity; IoT terminal side; safety protection; SM9 cryptographic algorithm

电力物联终端侧安全防护密码的研究背景涉及当前物联网技术的快速发展和广泛应用,以及电

力系统的基础设施网络安全问题^[1]。随着越来越多的终端设备连接到电力系统网络中,例如智能电

表、智能插座和智能家居设备等,这些终端设备成为可能遭受未经授权访问、信息泄露、篡改或破坏的潜在目标^[2]。因此,确保电力物联终端侧的安全性变得至关重要。

针对该问题,相关学者也提出了一些较好的研究成果。文献[3]将 Feistel 架构与 SPN 架构相结合,研究一种新型的基于非保密信道的轻型、可用于加密机密信息的新型对称块密码。当前,Feistel 结构被广泛运用于对称密码算法中,如 DES、AES 等,其主要缺点是在多轮加密过程中需要大量的轮函数和密钥调度,增加了硬件资源和算法复杂度,可能会导致性能下降,尤其是在对抗侧信道攻击时,Feistel 结构的设计问题容易受到攻击者的利用。文献[4]为了有效地保障移动终端的数据安全性,采用了一种基于动态证明的方式来检验密态文件的真实性,同时也实现了对密态文件的动态修正和渐进式的升级。动态证明方法是一种新型密码学技术,用以验证某些计算的正确性和安全性,在零知识证明和可验证计算方面具有重要应用。然而,动态证明方法的主要缺点之一是计算开销较高,特别是对于复杂的计算任务,生成和验证证明的过程会消耗大量的计算资源和时间,影响了系统的性能和效率。

为了进一步优化电力物联终端侧的接口数据和用户隐私数据的安全性,本文提出了新的密码算法。

1 电力物联终端

电力物联终端是指将物联网技术应用于电力系统中的终端设备,构成的一个以电力系统为基础的物联网网络。电力物联终端结构如图 1 所示。

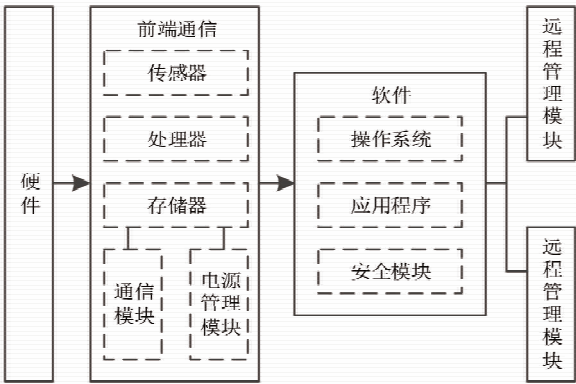


图 1 电力物联终端结构

1.1 硬件结构

①传感器:用于实时监测电力系统中的各种参数,如电压、电流、功率、温度等。传感器会收集这些数据并将其转化为数字信号,以便终端设备进行处理和传输^[5]。

②处理器:通常采用嵌入式处理器或微控制器,用于执行各种操作和算法,处理传感器采集的数据,并控制终端设备的运行。

③存储器:用于存储设备配置信息、用户数据、历史记录等内容。存储器可以采用闪存、SD 卡等形式,以保证数据的长期存储和安全性。

④通信模块:包括有线或无线通信模块,用于与其他电力设备或数据中心进行通信,实现数据的传输和接收。常见的通信技术包括 Wi-Fi、蓝牙、Zigbee 等。

⑤电源管理模块:负责管理终端设备的供电和功耗,确保设备正常工作,延长终端设备的使用寿命^[6]。

1.2 软件结构

①操作系统:提供硬件访问接口、任务管理、资源分配等功能,用于管理终端设备上的各种软件程序的运行。

②应用程序:包括数据采集、处理和传输程序,用户界面程序,控制算法等。这些应用程序根据具体需求设计实现终端设备的各种功能。

③安全模块:用于保护终端设备和通信数据的安全性,包括加密解密算法、访问控制、身份认证等功能。

④远程管理模块:用于远程监控、升级和配置终端设备,方便运维人员对设备进行管理 and 维护。

综上所述,电力物联终端的结构是一个综合硬件和软件的系统,通过各种组件相互配合,实现电力系统的监测、控制和智能化管理。不同的终端设备可能有着不同的硬件和软件结构,但通常都包含传感器、处理器、通信模块、存储器和软件应用程序等组件,以实现电力系统的采集、处理、传输和用户交互等功能。在整个系统中,安全模块扮演着至关重要的角色,保证电力物联终端的安全性和可靠性。

然而,随着电力物联终端的广泛应用,其安全性问题也日益突出,因此需要对电力物联终端侧进行安全防护密码研究。电力物联终端在通信过程中可能面临窃听、中间人攻击和数据篡改等威胁,这对电力系统的运行和用户的安全造成潜在风险。且由于电力系统属于国家基础设施的一部分,其安

全受到政府和用户的高度关注,因此需要确保电力物联终端的安全性。

2 电力物联终端侧安全防护密码算法设计

2.1 接口数据密码算法

电力物联终端侧接口数据密码算法的意义在于确保接口数据传输的安全性,包括机密性、完整性和认证性,有效防止数据泄露、篡改和恶意攻击。其重点在于设计和实现一种可靠的密码算法,加密和解密接口数据,同时保障用户隐私信息不被泄露,维护系统稳定性和安全性。由于电力物联终端侧过程易遭受恶意攻击,采用 SM9 密码算法^[7-8]对电力物联终端侧接口数据做加密处理,保证电力物联终端侧环境安全,流程如图 2 所示,具体步骤如下:

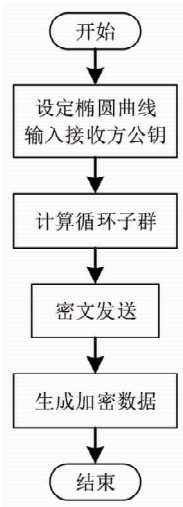


图 2 接口数据加密流程

SM9 密码算法是一种基于椭圆曲线密码学的公钥密码算法,专门用于数字签名、身份认证和密钥交换等应用场景。定义电力物联终端侧接口数据在有限域上的椭圆曲线 $Q(M)$,公式如下所示。

$$\begin{cases} y^2 = x^3 + ax + b \\ a, b \in W \\ x, y \in Q \end{cases} \quad (1)$$

式中, x 、 y 均表示椭圆曲线中的接口数据点; a 、 b 分别表示曲线的相关系数; W 表示有限域; Q 表示的是椭圆曲线。

在密码算法中,首先将网络节点一侧的界面信息转化为一个椭圆曲线上的一个子集,然后以此为参照点,求解出了一个椭圆曲线上的周期群 g_1 和 g_2 。公式如下所示。

$$\begin{cases} g_1 = \gamma_1 g \\ g_2 = g + \gamma_1 \end{cases} \quad (2)$$

式中, γ_1 表示电力物联终端侧接口数据节点所代表的消息。

通过将数据以 g_1 和 g_2 的形式加密发送给接收者,并在解密时仅需计算出恢复的明文数据,这个过程即为电力物联终端侧接口数据的加密。

采用 SM9 密码算法不仅可以提高电力物联终端侧环境的安全性,而且在破解所需的时间相同时,SM9 所需的密钥长度更短,并且效果更为优越。解密公式如下所示。

$$G = g_2 - \phi g_1 \quad (3)$$

式中, ϕ 表示明文解密系数。

基于上述内容,计算密文。在利用 SM9 密码算法加密电力物联终端侧数据时,计算密文的目的是增加数据的安全性和隐私保护。通过计算密文,可以将原始数据转换为一段不可直接理解的加密数据,从而有效隐藏数据的内容,使得未经授权的人无法轻易获取敏感信息。同时,计算密文还可以增加数据传输和存储的安全性,减少信息泄露的风险。对于电力物联终端侧数据这样涉及重要信息和隐私的数据,采用加密算法计算密文是非常必要的步骤。

利用密文和密文的映射生成乱序密文^[9]。生成乱序密文的过程中,首先通过对密文进行一定的映射操作,然后根据映射规则重新排列生成新的密文。这种乱序密文的生成方式可以增强数据的安全性和抗攻击能力。原理是通过对密文进行映射操作,改变密文的顺序或位置,使得原本相邻的密文在乱序后不再相邻,从而混淆数据的顺序和结构,增加了破解的难度。乱序密文的生成可以采用不同的算法和映射规则,如置换算法、置乱算法等,以实现数据的重新排列和混淆,从而增加数据的保密性。

这种乱序密文的生成对于信息安全领域具有重要意义。首先,乱序密文可以提高数据的隐蔽性,使得密文更加难以被解读和分析,增加了信息的保密性。其次,乱序密文增加了对数据攻击的抵抗能力,降低了黑客窃取数据或进行恶意篡改的风险^[10]。最后,乱序密文还可以增加数据传输和存储的安全性,进一步保障敏感信息的安全性。

选取两个维度为 χ 的加密密钥 i 和 j ,其共同构成的电力物联终端数据集合对为 $Q(\chi) = [(i_1, j_1), (i_2, j_2), \dots, (i_n, j_n)]$ 。设 P 为待加密的数据,将顺序密文的第 n 个子密文 P_n 映射为乱序

密文 P'_n, P_n 和 P''_n 满足:

$$P'_n = P_n - P''_n \quad (4)$$

由此得到加密密文为:

$$P = (P'_1, P'_1, \dots, P'_m) \quad (5)$$

为了优化数据加密的强度,在密文中加入随机误差向量。随机误差向量是一段随机生成的数据,与原始数据进行异或操作后加入密文中^[11]。这样做可以增加加密数据的随机性,使得密文更加难以被分析和猜测,提高了攻击者解密的难度。设定引入的随机误差向量为 η ,得到更新后的密文为:

$$\dot{P} = \eta \cdot \kappa / \Re \quad (6)$$

式中, $\Re$ 表示内积参数; κ 表示比特向量。

2.2 用户隐私安全防护

为了保护电网物联网终端一侧用户的个人信息,本节通过在电网感知的终端一侧产生一个随机数,并在此基础上对其进行加密,从而得到其中的公开密钥,以此为基础构建一个面向用户隐私信息的安全防护密码算法^[12-13]。

公式如下所示:

$$\begin{cases} U = G\delta^{H_{ID}} \\ \chi = [ID, G] \end{cases} \quad (7)$$

式中, U 代表用户的公开密钥; δ 代表密钥交换协议中的原根信息; H 表示公开密钥的防护码; U 为生成的随机数; χ 代表用户隐私安全标识与公开密钥构成的接口数据包^[14-15]; ID 表示用户的用户隐私安全标识。

电力物联终端侧接口数据加密与用户隐私安全防护完成后,防护双方即可使用公开密钥实现安全电力物联终端侧。用户隐私安全防护流程如图 3 所示,以用户 1 和用户 2 位用户隐私安全防护的对象,同时对用户 1 和用户 2 实施公开密钥处理,在双方公开密钥后同时完成身份标识,此时可获取具有身份信息的密钥,判断该身份密钥是否达到防护标准,如果确认满足防护条件,则说明此时完成了身份认证,如果不确认满足防护条件,则说明本次身份验证失败。

3 实验设计与结果验证

选择智能电表(图 4)作为实验测试环境,该电力物联终端设备,具有数据采集传输功能,并可与其他电力设备连接。智能电表作为连接电力系统和用户设备的重要节点,需要确保采集的用电数据传输过程中的机密性和完整性。同时,智能电表可能涉及用户的电力使用情况等隐私信息,需要对这些

些信息进行有效的保护。

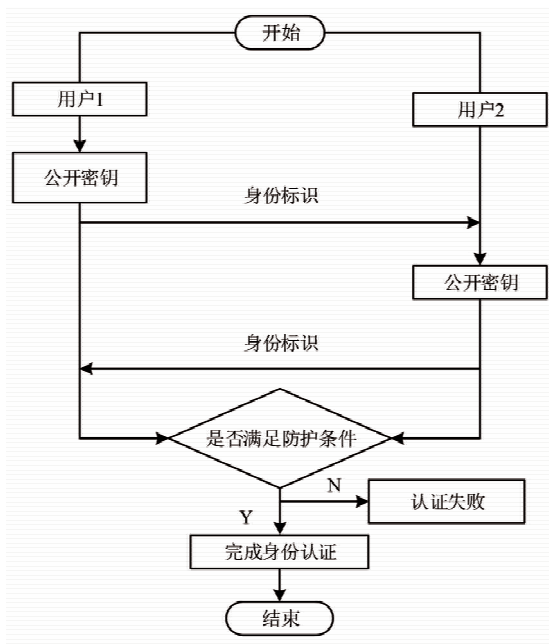


图 3 用户隐私安全防护流程



图 4 智能电表

基于智能电表,搭建一个安全的本地网络环境,该网络包括路由器、防火墙等网络设备。确保数据传输通道的安全性,防止数据被窃取或篡改。模拟用户信息的输入和管理,包括用户名、密码、身份验证等用户信息,用于测试安全防护密码算法对用户信息的保护效果。使用本文算法、文献[3]算法和文献[4]算法对终端设备和用户信息进行加密处理,以验证密码算法对数据的保护效果。

利用本文算法对电力物联终端侧接口数据完整性进行验证,并对比文献[3]算法和文献[4]算法的结果,具体如表 1 所示。

由表 1 中的数据可知,研究提出的电力物联终端侧密码算法应用下,接口数据的丢失率更低,当接口数据传递次数达到 60000 次时,数据的丢失率

为 0.26%，可满足实际应用要求。

以电力物联终端侧用户隐私数据的丢失率为指标，测试不同算法对用户个人信息的防护效果，结果如图 5 所示。

表 1 电力物联终端侧接口数据篡改结果

接口数据传递 次数/次	数据传输量/ MB	电力物联终端侧接口数据篡改率/%		
		本文算法	文献[3] 算法	文献[4] 算法
10000	5000	0	0.52	0.95
20000	10000	0	1.45	1.23
30000	15000	0	1.26	1.59
40000	20000	0	1.89	2.07
50000	25000	0.21	2.04	2.57
60000	30000	0.26	2.23	2.69

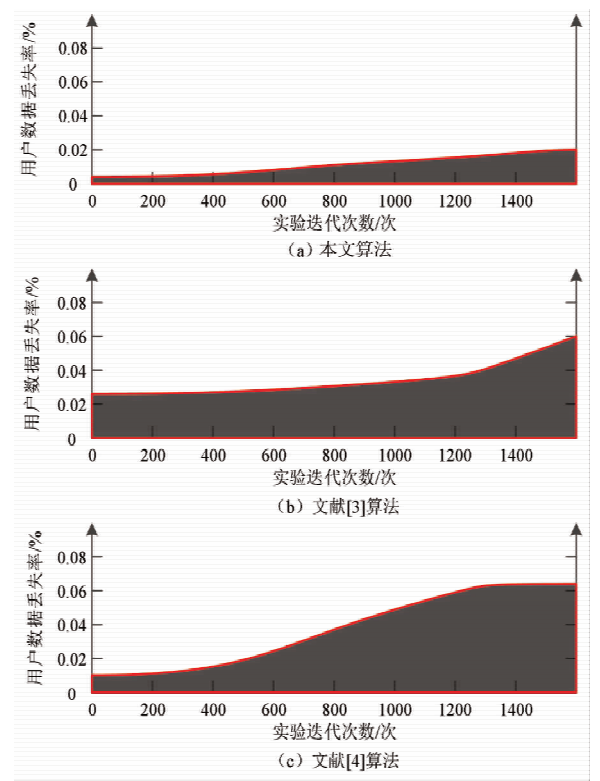


图 5 不同算法下用户隐私防护效果对比

由图 5 可知，与文献算法相比，本文算法应用后，电力物联终端侧用户隐私数据的丢失率始终低于 0.02%，用户隐私得到了较好的防护。电力物联终端侧用户隐私数据的丢失率无法降低至 0，主要是因为数据传输环节可能存在漏洞或不安全因素，终端设备本身可能存在安全缺陷，以及人为操作错误或恶意攻击等因素都可能导致用户隐私数据的丢失。综合考虑硬件、软件、网络和人因素，虽然可以采取各种安全措施降低数据丢失风险，但由于绝对的安全不存在，因此无法将用户隐私数据

的丢失率降至 0。

4 结 论

本研究通过采用 SM9 密码算法对电力物联终端侧接口数据进行加密处理，并结合用户的公开密钥和隐私安全标识设计了面向用户隐私信息的安全防护密码算法。实验结果表明，该算法应用下，接口数据和用户隐私数据的丢失率得到有效降低。这一研究为电力物联终端侧安全防护提供了一种新的解决方案，有望在确保数据安全性的同时提升系统性能和用户体验。

参考文献

[1] 严康,陆艺丹,覃芳璐,等.配电网用户侧异构电力物联设备网络风险量化评估[J].电力系统保护与控制,2023,51(11):64—76.

[2] 严康,陆艺丹,于超宗,等.配电网用户侧异构电力物联设备安全研究综述及展望[J].电力自动化设备,2023,43(3):146—158.

[3] 陈立军,蒋慧勇,Feistel 和 SPN 混合轻量级密码算法[J].大连工业大学学报,2023,42(4):288—298.

[4] 何佩,郑文斌,池晓金,等.电力物联网终端存储设备身份认证与数据保护方法研究[J].西北工业大学学报,2022,40(5):1188—1194.

[5] 李峰,陈亮,李凯,等.物联网安全标准体系框架研究[J].电子技术应用,2022,48(7):8—12.

[6] 赖建昌,黄欣沂,何德彪,等.基于商用密码 SM9 的高效分层标识加密[J].中国科学:信息科学,2023,53(5):918—930.

[7] 唐飞,凌国玮,单进勇.基于国产密码算法 SM9 的可追踪属性签名方案[J].电子与信息学报,2022,44(10):3610—3617.

[8] 王剑锋,林永峰.基于神经网络的电力调度信息加密传输方法研究[J].微型电脑应用,2022,38(1):134—138.

[9] 马海峰,王俊华,薛庆水,等.用户可实时撤销的云存储数据完整性验证方案[J].计算机工程与设计,2023,44(10):2943—2949.

[10] 马丽,姜火文,彭云.基于用户同意的隐私保护协议形式化描述与验证[J].电子学报,2023,51(7):1842—1849.

[11] 欧家祥,胡厚鹏,何沛林,等.基于国密算法的电网 AMI 数据安全防护技术[J].西南师范大学学报(自然科学版),2023,48(3):17—24.

[12] 彭婧,尹立夫,王洲,等.电力数据脱敏安全防护体系[J].计算机应用,2022,42(S1):191—194.

[13] 刘增毅,王琦,薛彤,等.电力系统中数据驱动算法安全威胁分析及应对方法研究[J].中国电机工程学报,2023,43(12):4538—4554.

[14] 蔡莹,朱翔,王舰,等.基于激光注入的 FPGA 加密防护设计验证研究[J].电子学报,2022,50(10):2381—2386.

[15] 王高洲,王惠剑,王聪,等.基于 SM2 密码算法的电力数据安全接入方法[J].南京理工大学学报,2022,46(6):749—755.