

# 基于IDEA与RSA算法的终端绑定现场数据验证方法

通过改进IDEA算法,将密钥中加入移动终端特有数据IMEI和IMSI,利用此算法加密所要传输的现场数据;并采用RSA算法加密IDEA算法中的密钥,利用IDEA与RSA算法的组合实现了密文和密钥的加密传输,并结合数据解密以及反馈验证技术,实现移动运维现场与远程系统间实时可靠的交互验证,有效监督现场的运维情况,为电力企业现场运维、远程支持、规范化管理和工作决策提供有效的辅助支撑。

周正<sup>1</sup> 陈家璘<sup>1</sup> 邵波<sup>2</sup> 戚娟<sup>2</sup>/1.国网湖北省电力公司信息通信公司  
2.国网电科院南瑞集团信息通信技术分公司



周正/高级工程师

## 关键词/Keywords

移动作业·  
IDEA算法·  
RSA算法·  
移动终端绑定·

## 0 引言

近年来,随着智能移动终端的发展,移动作业已广泛应用于各个行业。目前,在电力系统现场运维中,也采用移动智能终端对现场设备进行信息采集和处理,通过将数据传输到远程平台系统,实现移动运维现场数据采集<sup>[1-2]</sup>。

但是,现阶段在现场移动运维作业中,一方面由于采用运营商提供的无线公网进行数据传输,并且对移动终端设备缺乏有效的安全管理保障,无法保证终端设备的接入和使用安全,更容易造成数据泄露,对电力企业安全生产造成隐患;另一方面,现场移动运维作业由于远离管理中心,缺乏有效的监督和管理,而现有的运维模式,缺少实时的现场运维数据验证功能,无法实现现场运维的闭环管理,无法确保现场人员是否按照要求规范、准确、有效的完成了现场运维工作。

本文提出了一种基于IDEA与RSA算

法的终端绑定移动运维现场数据验证方法,通过改进IDEA算法,将密钥中加入移动终端特有数据IMEI和IMSI,利用此算法加密所要传输的现场数据;并采用RSA算法加密IDEA算法中的密钥,利用IDEA与RSA算法的组合实现了密文和密钥的加密传输,并结合数据解密以及反馈验证技术,实现移动运维现场与远程系统间实时可靠的交互验证,有效监督现场的运维情况,为电力企业现场运维、远程支持、规范化管理和工作决策提供有效的辅助支撑<sup>[3-6]</sup>。

## 1 移动运维现场数据验证工作流程设计

本文设计的移动运维现场数据验证工作流程如图1所示,运维现场通过安全智能终端进行数据采集,采集的数据结合终端的特征数据采用IDEA和RSA算法完成数据加密,通过无线公网进行加密传输,而后传递到远程平台系统,系统通过数据解密、验证以及处理终端的请求,将处理结果再次加密回传至智能终端,完成验证工作流程。此流程主要包含以下4部分。

### (1) 数据采集管理

数据采集主要是对现场运维数据的采集,是加密传输、验证的重要先决条件。采用RFID、二维码识别技术、IODF(智能光纤配线架)、图像识别以及终端自带的GPS定位,实现移动运维数据的多样化采集。通过终端智能采集,有效提高了电力移动运维数据的时效性、规范性和准确性。

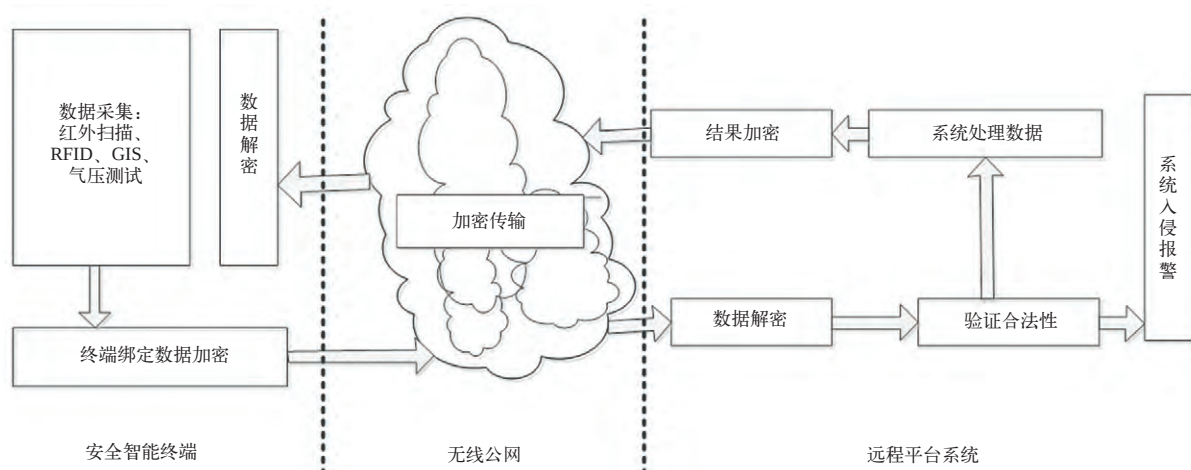


图1 验证工作流程图

## (2) 终端绑定管理

为了保证远程系统对现场运维接入终端的身份认证,以及增强运维数据的安全性,防止一卡多用和黑客攻击等,采用终端和远程系统绑定技术。利用每台终端所具有的唯一移动设备国际身份码IMEI和终端所插入的国际移动用户识别码IMSI两组识别码作为数据加密的部分密钥,在远程系统接收到终端数据接入时,通过数据解密,根据系统绑定的两组识别码,完成对接入终端的识别验证,保证了通过无线公网接入系统并进行数据交换的安全性和可管理性。

### (3) 数据加密、解密、验证管理

IDEA算法的安全性强且加/解密速度快，因此选择此算法加密采集的数据；另外，因其密钥中加入了终端特征数据IMEI和IMSI，而且其密钥量大，管理困难，因此采用RSA算法传递密钥，大大简化了密钥管理的难度，同时在远程平台解密时，首先解密密钥，验证合法性，对于非法密钥，无需解密采集数据的密文，可以降低风险，提高解密的效率。在此方法中，具体模块包括：现场采集数据加密、远程系统数据解密、远程验证、结果数据加密和终端接收数据解密。从而实现安全可控环境下完整的闭环化现场运维采集数据的验证管理。

#### (4) 数据传输管理

数据传输主要是利用无线公网实现终端设备和远程平台系统的点对点数据实时传输,包括现场采集数据传输至远程平台和远程平台验证信息

回传至终端两个部分。如图2所示。

## 2 主要关键技术

在以上流程设计的基础上,为实现现场数据验证方法的安全和高效,主要研究以下关键技术。

### (1) 加密、解密算法流程设计

为实现数据安全传输和终端绑定的管理，用IDEA算法来加密采集的明文数据，而同时使用RSA算法中公开密钥密码体制来传送IDEA的密钥。

加密过程为：一方面，包含终端数据IMSI和IMEI的128位IDEA密钥对采集的数据进行加密，得到密文C1；另一方面，终端获取远程平台发送的公开密钥，对IDEA的密钥进行RSA算法加密，得到密文C2；最后，C1和C2组合成密文C，通过无线公网传输到远程平台。

解密过程为：远程平台首先将收到的密文C拆分成C1和C2；然后用RSA的私有密钥解密C2，恢复出128位的IDEA算法密钥，验证IMSI和IMEI是否合法；最后，将合法的密钥对C1进行解密，恢复出明文。

## (2) IDEA算法子密钥生成

在IDEA算法的密钥中，需加入终端特征数据IMEI和IMSI，以实现终端绑定管理。IDEA算法加密和解密都需要输入128位密钥，输出52组16位的子密钥。加密子密钥的生成过程是：首先根据用户设定的密钥长度，利用伪随机数发生器产生一

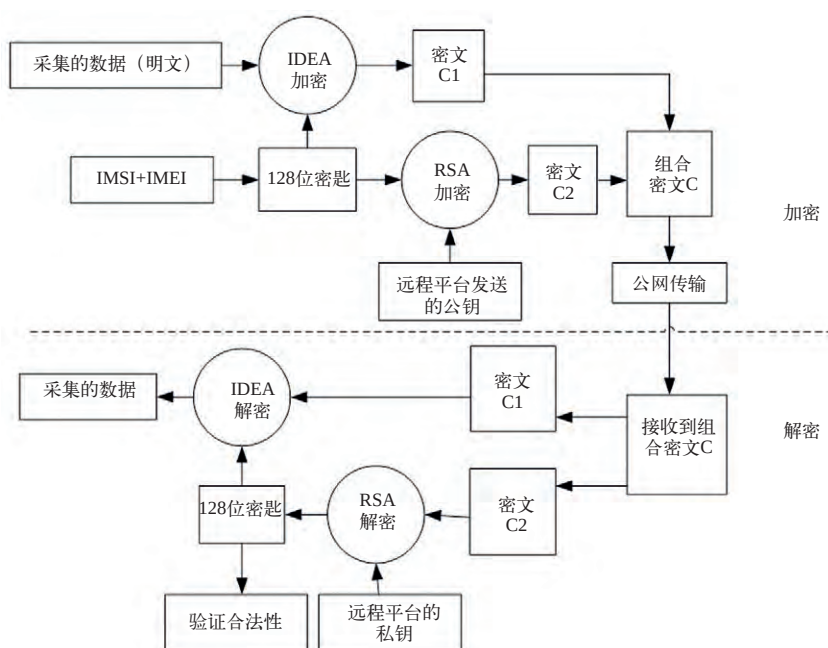


图2 加密、解密算法流程

组128位的伪随机数；然后将128位密钥分成8组，每组16位，从而得到8个子密钥。随机选择密钥中的任意2组16位密钥，分别用IMEI和IMSI进行替换，其中IMEI和IMSI各15位，另外一位由系统自动生成，即可得到新的8组子密钥。将此8组128位密钥循环左移25位，再做一次16位分组，又可得到8个子密钥，如此循环7次，在第7次循环中，只取前面4组密钥，便产生了全部的52组16位子密钥，具体流程如图3所示。

解密子密钥的过程是：首先对子密钥进行换位操作，然后进行部分子密钥的模216的加密逆运算和剩余部分子密钥的模 $(216+1)$ 的乘法逆运算。

### (3) IDEA算法加密、解密

加密过程是对52个子密钥和分组长度是64位的明文数据进行处理。64位被分为4个16位的子

块：X1、X2、X3、X4作为第一轮输入，每一轮中，将4个输入子块与6个16位子密钥分别做模216的加法、模216+1的乘法、异或操作，得到4个输出作为下一次的输入。如此共进行8次，最后用4个子密钥作输出变换，从而得到最后的密文。如图4所示。

解密过程是加密过程的逆。由于在加密中加入了IMEI和IMSI的参数，所以数据解密的同时还将验证数据的合法性，合法数据才能进行处理，未通过验证的数据将直接丢弃，并产生报警。

## 3 性能测试

为了保证此方法的可用性，对本方法进行了性能测试，测试环境为：CPU酷睿i3 3.3 GHz，内存4 G，操作系统RedHat，软件工具java。测试结果如表。

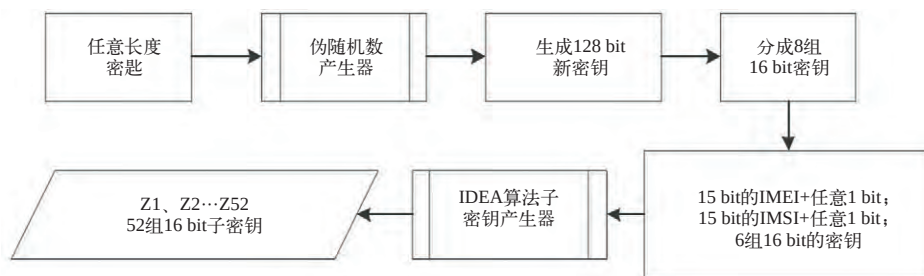


图3 子密钥的生成过程

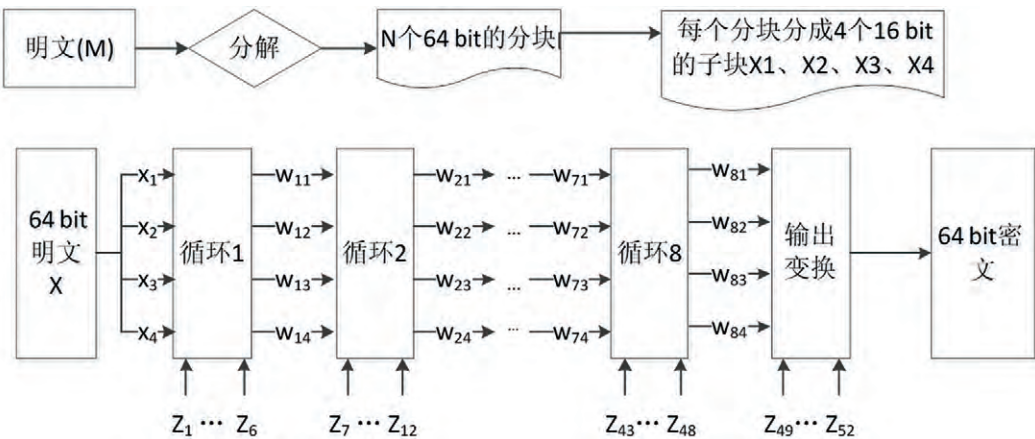


图4 IDEA加密算法

表 性能测试结果

| 项目       |              | 数值         |
|----------|--------------|------------|
| SM1加解密   |              | 7.7 Mbps/s |
| RSA公钥运算  | 1 024位(带CRT) | 330次/s     |
| RSA私钥运算  | 1 024位(带CRT) | 0.4 s/次    |
| RSA密钥产生  | 1 024位(带CRT) | 1.2 S/对    |
| IDEA公钥运算 | 1 024位(带CRT) | 330次/s     |
| IDEA私钥运算 | 1 024位(带CRT) | 25次/s      |
| IDEA密钥产生 | 1 024位(带CRT) | 260 ms/次   |

通过测试可以明显发现RSA算法的私钥运算和密钥产生是限制整体性能的重要指标，但是RSA加密的安全性能相对于IDEA加密要更好一些，所以在实际应用中采用了RSA算法加密IDEA算法中的密钥，因此能够在保证安全性的情况下有效提高加密速度。

4 结束语

本文通过将终端特征数据绑定到IDEA算法中，并结合RSA算法，完成运维现场数据的加密、解密、验证和回传功能，实现在终端至远程系统之间，不依赖于运营商加密机制构建了一条高强度的数据加密隧道，充分保证了数据传输的安全性和数据交互验证的可靠性。下一步可研究

将该方法应用于电力移动作业PDA接入系统中，以提高电力系统现场移动运维中更专业和安全的

管理。

参考文献

[1]张金玲, 黎峰, 刘镇顶.基于PDA的移动作业标准化管理系统[J], 计算机工程与设计, 2008, 29(7):1 831-1 833.

[2]秦超, 张涛, 林为民.电力移动作业PDA安全接入系统设计与实现[J], 电力系统自动化, 2012, 36(11):82-85.

[3]叶红, 李素, 郝建强.组合数据加密算法的研究与实现[J], 北京工商大学学报, 2007, 25(6):62-64.

[4]吴伟彬, 黄元石.IDEA算法的改进及其应用[J], 福州大学学报, 2007, 12(32):28-31.

[5]魏国珩, 周学广, 徐建桥.基于IDEA算法的数据软加密性能分析[J], 计算机与数字工程, 2007, 35(17):62-63.

[6]肖四友.基于X-IDEA算法实现手机通信中图文加密[J], 计算机系统应用, 2011, 20(4):227-230.

(收稿日期: 2015-05-25) EA

作者简介

周正 (1980-), 男, 博士, 高级工程师, 主要研究方向为信息通信调度运行监控与资源管理。

陈家璘 (1985-), 男, 硕士, 工程师, 主要研究方向为信息通信系统管理。