「配电网」

基于国密算法的智能移动终端的研究与实现

文/北京国网信通埃森哲信息技术有限公司　刘　暘
国网厦门供电公司　洪　汛
厦门亿力吉奥信息科技有限公司　李永海　李　琦

为了全面推行以新技术带动配电网发展的模式，实现“创建国际一流城市配电网”的重要目标，电网现场作业应全面应用云计算、大数据、物联网和移动互联等新一代信息通信技术，建成“互联网＋移动作业”工作体系，促进现场管理模式向多样化与智能化的方向转变，形成人员管理、业务管控以及应急指挥的移动化、信息化和网络化，大力提升公司的互动化管理水平。

国密算法研究

1. SM1对称密码

SM1 算法是分组密码算法，分组长度为128 bit，密钥长度都为 128 bit，算法安全保密强度及相关软硬件实现性能与 AES 相当，算法不公开，仅以 IP 核的形式存在于芯片中。

采用该算法已经研制了系列芯片、智能 IC 卡、智能密码钥匙、加密卡、加密机等安全产品，广泛应用于电子政务、电子商务及国民经济的各个应用领域（包括国家政务通、警务通等重要领域）。

2. SM2椭圆曲线公钥密码算法

SM2算法就是ECC椭圆曲线密码机制，但在签名、密钥交换方面不同于ECDSA、ECDH等国际标准，而是采取了更为安全的机制。另外，SM2推荐了一条256 bit的曲线作为标准曲线。

ECC椭圆曲线密码体制Koblitz和Miller在1985年各自引入密码学。椭圆曲线的Weierstrass方程为，其上面的所有点和无穷远点构成一个加法交换群，其中无穷远点是加法零元。此群的加法法则可以由弦切法所给出，具体见图1。

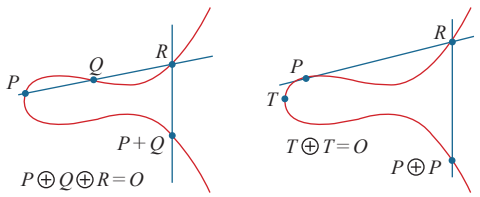

图1　SM2椭圆曲线公钥密码算法

图1中是两个不同点P和Q的加法，右图为相同的点P和P的加法。由弦切法便可以给出椭圆曲线上的加法方程。多倍点运算是指：给定一点P和一个整数k，计算kP，即k个P点的和。椭圆曲线上的离散对数问题为：给定点P和kP，计算整数k。椭圆曲线密码体制的安全性便是建立在椭圆曲线离散对数问题之上。

SM2标准包括总则，数字签名算法，密钥交换协议，公钥加密算法四个部分，并在每个部分的附录详细说明了实现的相关细节及示例。

SM2算法主要考虑素域和上的椭圆曲线，分别介绍了这两类域的表示，运算，以及域上的椭圆曲线的点的表示，运算和多倍点计算算法。然后介绍了编程语言中的数据转换，包括整数和字节串，字节串和比特串，域元素和比特串，域元

素和整数，点和字节串之间的数据转换规则。详细说明了有限域上椭圆曲线的参数生成以及验证，椭圆曲线的参数包括有限域的选取、椭圆曲线方程参数、椭圆曲线群基点的选取等，并给出了选取的标准以便于验证。最后给出椭圆曲线上密钥对的生成以及公钥的验证，用户的密钥对为（s，sP），其中s为用户的私钥，sP为用户的公钥，由于离散对数问题从sP难以得到s，并针对素域和二元扩域给出了密钥对生成细节和验证方式。

3. SM3杂凑算法

SM3密码杂凑算法给出了杂凑函数算法的计算方法和计算步骤，并给出了运算示例。此算法适用于商用密码应用中的数字签名和验证，消息认证码的生成与验证以及随机数的生成，可满足多种密码应用的安全需求。在SM2，SM9标准中使用。此算法对输入长度小于2的64次方的比特消息，经过填充和迭代压缩，生成长度为256 bit的杂凑值，其中使用了异或、模、模加、移位、与、或、非运算、由填充、迭代过程，消息扩展和压缩函数所构成。具体算法及运算示例见SM3标准。

4. SM4对称算法

此算法是一个分组算法，用于无线局域网产品。该算法的分组长度为128 bit，密钥长度为128 bit。加密算法与密钥扩展算法都采用32轮非线性迭代结构。解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。此算法采用非线性迭代结构，每次迭代由一个轮函数给出，其中轮函数由一个非线性变换和线性变换复合而成，非线性变换由S盒所给出。

5. SM7对称密码

SM7算法，是一种分组密码算法，分组长度为128 bit，密钥长度为128 bit。SM7的算法文本目前没有公开发布。SM7适用于非接IC卡应用包括身份识别类应用（门禁卡、工作证、参赛证），票务类应用（大型赛事门票、展会门票），支付与通卡类应用（积分消费卡、校园一卡通、企业一卡通、公交一卡通）。

6. SM9非对称算法

SM9是基于对的标识密码算法，与SM2类似，包含四个部分：总则、数字签名算法、密钥交换协议以及密钥封装机制和公钥加密算法。在这些算法中使用了椭圆曲线上的对这一个工具，不同于传统意义上的SM2算法，可以实现基于身份的密码体制，也就是公钥与用户的身份信息即标识相关，从而比传统意义上的公钥密码体制有许多优点，省去了证书管理等。

综上所述，智能移动终端在开展外网数据传输至内网时，采用了SM4加密算法。

系统架构研究

1. 头戴式可视设备在运检中的应用及关键技术研究

借助移动互联网技术，打造面向一线生产人员的智能移动终端，建立内外网数据安全交互通道，满足电网运行、设备状态、配网抢修态势等信息的内外网共享需求。系统整体架构如图2所示。

2. 智能移动应用

智能移动应用基于内网安全接入平台移动客户端支撑组件，实现现场任务管控、现场点到、事件上报、通信协作、远程调阅、移动地图、精准导航等功能，为一线人员提供全面、可靠的作业智能化支持。智能移动应用内置移动终端安全防护套件，可以远程控制终端数据，增强非法入侵、盗窃、丢失等的安全防护。为使系统后续能应用于日常作业，延续系统成果，智能移动应用对关键模块做了扩展接口处理，可以快速改造、切换，以集成其他功能模块、移动应用及业务系统等。

3. 智能移动应用安全接入

根据《国家电网公司关于加强和规范移动应用建设工作的通知》（国家电网信通〔2016〕684号）的有关要求，智能移动应用安全接入采用内网安全接入平台，由内网移动平台提供运行支撑。内网移动应用平台为各业务域内网移动应用提供统一的开发、管理和运行服务，实现内网移动应用、移动专控终端的统一管理和安全接入，同时对各应用公共功能进行统一建设，支撑面向内部员工的移动作业类应用的开发、管理、运行。

4. 智能生产指挥系统

智能生产指挥系统通过集成现场智能设备、原有应用以及统推应用，综合民政、公安、气象、交通等多源异构数据，利用整合通道实现各系统的信息交互与数据融合，并在此之上基于微应用框架，实现实施监控、研判预警、保电指挥、分析评价等功能，提升物资、车辆等自动化调配，构建一体化生产指挥控制平台，实现信息的全景可视化展现。

核心功能介绍

1. 任务调度

（1）现场任务管控

在智能移动终端智能化提醒指挥中心下发的生产任务，根据任务紧急程度、要求完成时间等优化待办任务管理。一线工作人员可实时了解工作内容，查看详细要求，并反馈工作信息。

（2）现场设备管控

借助智能移动终端内置或外置识别装置，辅助现场人员在现场智能识别任务设备，支持RFID、条码、二维码、铭牌等不同的识别方式。现场人员可以通过智能移动终端所携带的识别装置，自动采集各种信息或接受人工填报，并结合电网设备空间信息，实现现场电力设备数据采集。

2. 现场协作

（1）现场点到

实现远程点到功能，指挥中心发出点到指令，现场人员使用智能移动终端进行报到，报到时自动汇报当前位置、作业任务等，可实时确认保电人员就位情况、作业情况。

（2）事件上报

现场人员借助智能移动终端对区域内的供电电源、监测点运行数据进行监控，现场负荷参数异常（电压、电流、温度等）时，可以第一时间将异常事件上报到指挥中心。指挥中心根据上报的信息做出相应决策，将处置任务和相关资料下发到移动设备上，全程跟踪事件处置过程并实时上报事件状态。

（3）通信协作

实时收集、更新工作相关人员、机构信息，形成黄页，为一线人员提供详实的专项工作组通讯录，方便快速联系相关责任人。实现指挥中心及一线人员在电力无线虚拟专网、信息内网之间的点对点通信、内外网通信、群组会话等企信沟通，实现语音、图片、视频等多媒体数据的传送，可实时传递现场状况、操作台指令等信息，以支持指挥中心的远程指挥和专家指导，有效监控、指导现场作业。

（4）远程调阅

通过智能移动终端，一线人员可以实时查询区域内的接线情况，调阅接线图；可以实时查询

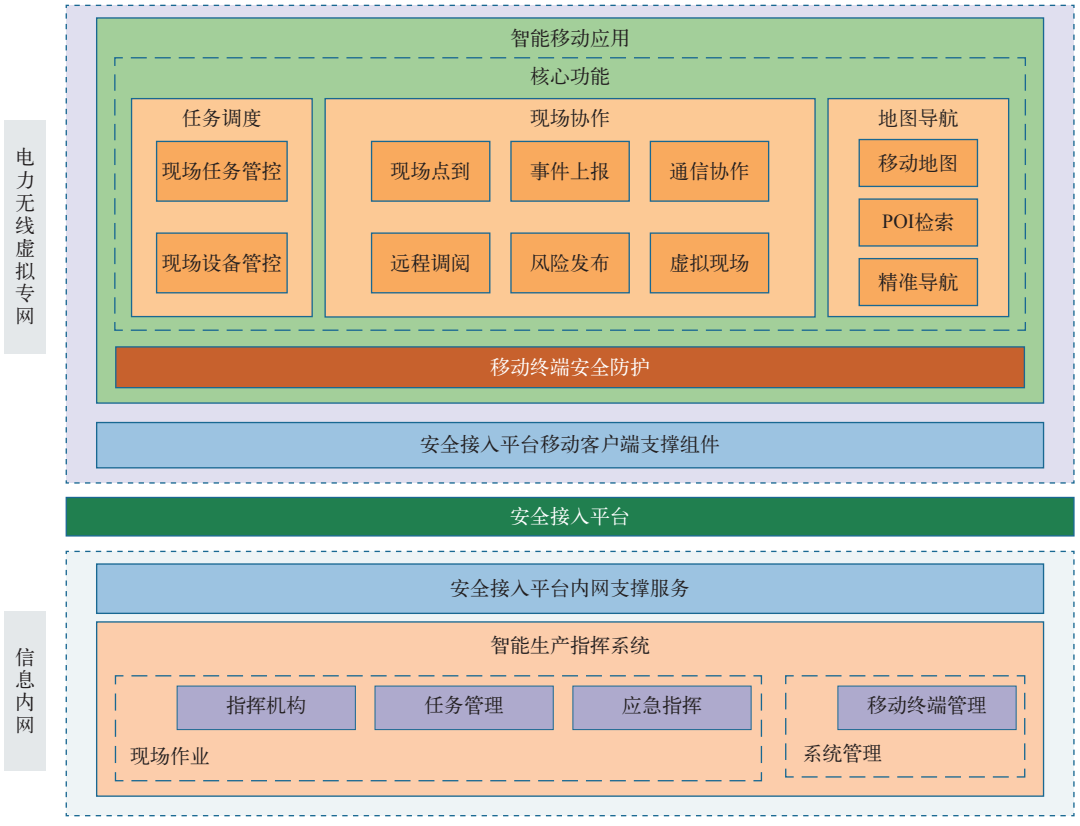

图2　系统架构

区域内的运行情况，调阅运行数据；可以实时查询任务信息，调阅应急预案，并可智能化提供指定设备相关预案。

（5）风险发布

当指挥中心发现相关监控预警信息时，或有专家研判信息时，主动向相应区域内的现场智能移动终端发布风险预警，提醒现场做好风险防护，及时排查隐患。

（6）应用集成

智能移动应用对关键模块做了扩展接口处理，如应用集成接口、身份认证接口、消息服务接口、数据同步接口等，可充分利用基于移动互联技术的可穿戴设备集成的体感传感器、智能眼镜、智能手环及相关可扩展传感器组件，实现与智能移动应用的集成，以支持语音输入、语音指令识别、手势指令识别等综合应用。

（7）虚拟现场

系统利用三维快速精确建模技术模拟现场场景，并依托AR/VR技术实现虚拟现场的沉浸式体验，保电专家可以通过系统及VR头显360°全景查看现场虚拟环境，展现各设备实时运行数据，并可模拟操作设备，以支持为保电作业提供作业指导及预警预判。

3. 地图导航

（1）移动地图

智能移动应用内嵌移动地图，搭载电网设备空间资源数据，支持基础导航地图渲染、自定义专题地图渲染，支持2D、3D地图，支持GPS/北斗＋基站＋Wifi多模式的混合精准定位，为一线工作人员提供电力设备分布、实时路况、气象预警等信息的可视化展示。

（2）POI检索

智能移动应用支持POI（兴趣点）精准搜索及周边查询与定位功能，搜索结果支持基于移动地图的定位展示。结合行业领域特点，可支持融合垂直领域的POI专题信息的查询与检索。

（3）精准导航

智能移动应用通过加载电网设备空间数据，定位任务目标设备，并结合最新的路网数据进行车辆行驶路径的规划，提供距离最短、道路等级、路口最少等多种导航方案，辅以实时智能语音导航，引导一线保电人员在第一时间到达作业现场。

4. 移动终端安全防护

移动终端安全防护套件包括远程锁定、远程擦除、短信指令、终端找回、数据备份等服务，可以在终端失窃等情况下远程锁定设备或远程清除设备数据，减少损失，防止事态升级。

入网检测，检测终端是否注册、终端安全策略是否应用、终端是否ROOT、终端是否有违规应用、终端是否启用违规功能等，对终端进行入网前的安全检测。

指纹识别，利用生物特征识别技术及独立密文存储固件，确保身份鉴别的唯一性、保密性。

SIM卡锁，提供SIM卡变更时自动锁定应用、后台自动报警功能。

远程锁定，设备失窃情况下，第一时间远程主动锁定应用，确保应用无法被他人使用，保护企业数据安全。

远程擦除，远程主动擦除终端上的应用数据，用于终端确认丢失或不再继续使用的情况。

短信指令，支持接收特定号码的短信指令，自动执行相应锁定、擦除、定位等指令，以在终端不联网的情况下仍能远程操控终端。

数据备份，实现用户关键数据的远程备份，可从备份服务器恢复到别的办公终端。

终端找回，自动跟踪终端的最后定位位置，为找回终端提供地理位置范围。

结束语

1. 深化生产指挥移动领域应用

系统与生产指挥系统紧密结合，深度整合现场应用，支持各种作业任务类型管理，可快速集成巡检、抢修等业务系统应用，共享各业务领域数据，实现现场信息全景化展示，达到一次任务、多系统联动效果。

2. 提升应急预案智能化、精准化

系统提供远程调阅功能，实现作业指导书、应急预案等作业资料查询，形成嵌入式移动现场作业资料库，可根据设备智能提供精准应急预案及作业指导，快速过滤无关内容，有效提升应急预案智能化、精准化水平。

3. 积极探索保供电现场虚拟指挥

系统通过集成AR/VR技术实现虚拟现场，为现场作业提供预先场景模拟及操作模拟，有助于提前发现缺漏事项，增强现场作业安全防护。**EA**

（收稿日期：2017.10.10）

（编辑：白文亭）