



基于组合密钥的智能电网多源数据安全保护

高建, 陈文彬, 庞建民, 于华东, 宋国瑞
(北京智芯微电子科技有限公司, 北京 102200)

摘要: 电力通信网是电力系统的重要基础设施, 对于数量庞大、分布广泛的各类业务终端、通信终端, 其数据保护关系着整个电网的安全稳定运行。如何解决大量节点需要的大量密钥问题, 避免大量节点因密钥不足而无法安全交换信息的情况, 提出基于密钥的分片组合技术实现有限密钥的扩展, 基本思想是根据不同条件获得分片方案, 把一个密钥分成若干个互不相同的子密钥片, 然后把这些密钥分片组合生成新的密钥, 分配到系统中的不同终端上。足够的对称密钥有利于密钥更新, 可以保证数据业务一次一密, 可有效增强通信系统抗破坏和抗入侵的能力。通过分析计算, 进一步验证了该方法在利用有限密钥实现大量终端业务数据保密传输中的有效性。

关键词: 配用电大数据; 通信安全; 多源数据; 密钥分片组合

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2020002

Multi-source data security protection of smart grid based on combination key

GAO Jian, CHEN Wenbin, PANG Jianmin, YU Huadong, SONG Guorui
Beijing Smartchip Microelectronics Technology Co., Ltd., Beijing 102200, China

Abstract: As an important infrastructure of power system, power communication network has deployed a large number of widely distributed business terminals and communication terminals, whose data security is related to the safe and stable operation of the entire power network. In order to avoid the situation that the information cannot be safely exchanged due to the shortage of keys. The sharding and combination technology based on keys was proposed to realize the expansion of limited keys, so as to solve the problem of a large number of keys needed for multi-node and multi-service. Firstly, a sharding scheme was obtained according to different conditions. A key was divided into several different sub-key pieces, and then a new key was generated by combining these key pieces and distributed to different terminals in the system. A large number of combined keys generated were conducive to update key, which could ensure the data service "one at a time" and effectively enhance the communication system's ability to resist damage and invasion. Through analysis and calculation, the effectiveness of this method in realizing real-time update of a large number of terminal business keys with limited keys was further verified, and data secure communication was realized.

Key words: power distribution and utilization, communication security, multi-source data, quantum key distribution

1 引言

为了适应配电自动化、用电信息采集、分布式能源等智能化业务系统,电网公司部署了数量庞大、分布广泛的各类业务终端、通信终端。对于点多面广、环境开放的各类终端,安全防护措施相对薄弱。并且攻击者能够通过终端迂回攻击主站,造成更大范围的安全威胁^[1-2]。

传统密码学的安全性基于数学算法的计算复杂度,随着分布式计算和量子计算机的愈加成熟,已不能保证密钥的绝对安全性。结合室外充电站、站所终端 DTU、配变终端 TTU、馈线终端 FTU、智能电表等终端特点,实现配用电终端安全、高效、可靠地响应业务安全的需求,具有重要实用价值^[3-4]。Kumar 等^[5]提出了安全通信的轻量级弹性协议,但是该协议正常运行的前提是初始化密钥始终安全有效,其一旦泄露就会直接影响数据的安全传输。刘国荣等^[6]提出了云端协同运算的数据加密技术方案,将数据加密过程、密钥信息分别在云端、终端运算和存储,没有充分考虑智能电网中通信终端的存储空间和计算能力。Xiao 等^[7]提出了一种动态对称密钥算法,网络状态对算法的影响程度较大,动态密钥存储的是整个数据分组,存储空间极大。潘涛等人^[8]提出数据聚合技术,在加密用户数据后再进行聚合,虽然比传统的聚合方法效率高,但聚合步骤增加相应的成本和设备负担。

本文提出基于密钥的分片组合技术,并将其与数据业务的可靠性相结合,利用有限的密钥高效生成大量新的密钥,然后把这些密钥分配到系统中的不同终端上,满足配用电业务端到端的安全防护需求,实现保密通信技术在配用电业务的低成本、大规模应用。

2 电力通信网数据安全需求

电力通信网是一个信息化和数字化的网络,

它的安全稳定运行是确保电力生产、配送的关键。电力通信网中的安全需求可分为 4 个方面:数据的保密性、消息的完整性、不可抵赖性和可用性。为了保证电力系统的安全,需要特别关注电网数据的信息安全,确保总部与各调配站、各单位之间信息传输的安全进行,保护信息不被窃取或被不相关人员看到^[9-10]。

利用保密通信技术进行配用电业务身份认证、数据加密等环节所需密钥的分发,并探索与现有安全防护措施之间的兼容机制,对于提升配用电业务信息安全防护能力具有重要意义。

3 实现方法设计

3.1 方案流程

提出一种适用于配用电业务的密钥分片组合应用方法,方案是利用初始密钥作为种子密钥,通过分片和组合技术,将这些种子密钥映射成大量的对称密钥,以实现大量终端的数据加密通信,弥补密钥生成分发速率较低的缺陷,满足点多面广的配用电终端所需的大量高安全性密钥的需求。

首先从密钥生成设备中读取量子密钥实时成码率,对密钥实时成码率和预设时长进行相乘运算,确定总密钥量资源。同时统计所在地区的终端数量以及密钥更新速率,获取终端所需的密钥数量。通过对比总密钥量和所需的密钥量,计算得到密钥的分片方式、分片段数,然后利用密钥组合公式生成新的量子密钥,实现对终端业务的数据加密,满足终端对大容量密钥的需求。具体流程如图 1 所示。

3.2 密钥分片

密钥分片的方法是把一个密钥分成 m 个不同的片组,称为 m 个子密钥,设定共有 n 个密钥,经分片后形成的子密钥资源数量 $L=mn$ 。然后把这些片或片组的子密钥进行唯一标识,用于密钥的组合从而生成相对应的密钥。密钥分片方式可采用两段至多段的方式,优选地采用两段或三段的方式。两段



和三段分片方式示意分别如图2、图3所示。

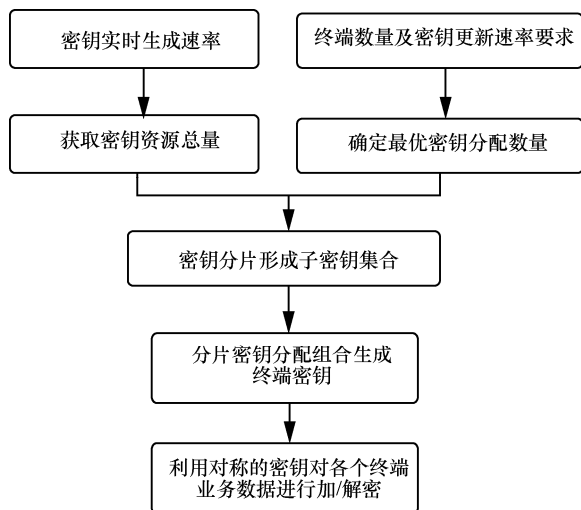


图1 密钥分片组合应用方法流程

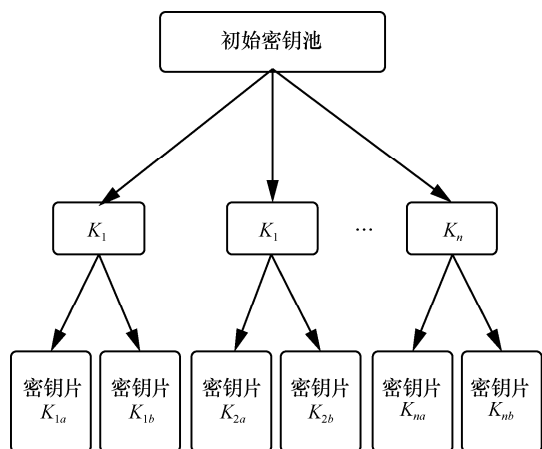


图2 两段分片方式示意

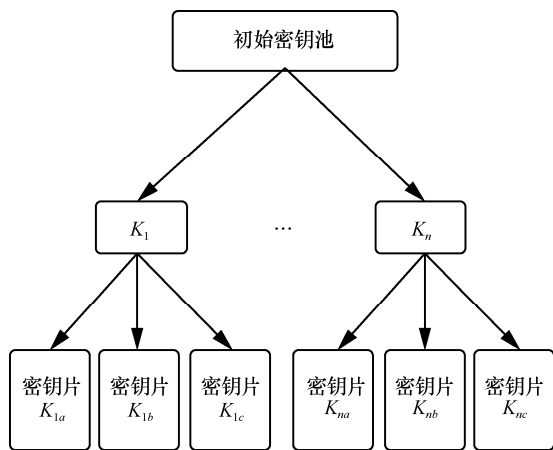


图3 三段分片方式示意

分片数量通过式(1)进行确定, 先将密钥的

生成数量与终端所需要的密钥数量进行对比, 确定密钥的分片数量, 不同的分片数量与所对应的总的可生成的密钥数量之间的关系为:

$$K_{\text{总}} = C_{mn}^m = C_L^m \quad (1)$$

以两段分片为例, 密钥池有 n 个密钥, 两段分片后共形成 $2n$ 个子密钥, 子密钥集合:

$$R = \{K_{1a}, K_{1b}, K_{2a}, K_{2b}, \dots, K_{na}, K_{nb}\} \quad (2)$$

考虑密钥的组合可以产生 C_{2n}^2 个组合密钥, 而且这些密钥都是不相同的, 具备了两个不同量子密钥的特性, 安全性更好。

进一步以三段分片为例, 分片后共形成 $3n$ 个子密钥, 考虑密钥的组合可以产生 C_{3n}^3 个组合密钥。可结合终端的数量和密钥的更新速率确定密钥的分片段数。

使用密钥分片主要是为了在有限量子密钥的情况下, 生成足够的量子密钥, 为密钥的组合生成提供基础, 从而提高密文安全性。

3.3 密钥组合

通过密钥因子矩阵依次随机从集合 R 中选取与分片数量对应的没有重复的元素, 组合生成密钥。密钥因子矩阵的元素可由服务器采用硬件随机数发生器生成方法或软件系统的伪随机数产生散列函数生成, 密钥因子矩阵 T_K 表示为:

$$T_k = \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1j} \\ r_{21} & r_{22} & \dots & r_{2j} \\ \dots & \dots & \dots & \dots \\ r_{i1} & r_{i2} & \dots & r_{ij} \end{bmatrix} \quad (3)$$

矩阵的行表示组合密钥的每一段包含的密钥变量, 矩阵的列表示组合密钥的段数, 设矩阵为 i 行 j 列的密钥因子矩阵, $i=mn$, $j=m$, i 行是从子密钥集合中选取的有效子密钥, j 列表示组合密钥运算的段数。

用散列函数将密钥片标识映射成矩阵的行和列, 再提取矩阵的行与列所对应的密钥因子来进行组合, 即生成相对应的密钥。对应实体标识 ID

的密钥,子密钥集合在密钥因子矩阵的每一列选取的密钥因子为 K_m :

$$K_m = (k_1, k_2, \dots, k_L) \begin{pmatrix} r_{1m} \\ r_{2m} \\ \dots \\ r_{Lm} \end{pmatrix} \quad (4)$$

则 ID 的密钥为:

$$K_{ID} = (K_1 + K_2 + \dots + K_m) \bmod q \quad (5)$$

$$K_{ID} = (k_1, k_2, \dots, k_L) \begin{pmatrix} r_{11} \\ r_{21} \\ \dots \\ r_{L1} \end{pmatrix} + (k_1, k_2, \dots, k_L) \begin{pmatrix} r_{12} \\ r_{22} \\ \dots \\ r_{L2} \end{pmatrix} + \dots + (k_1, k_2, \dots, k_L) \begin{pmatrix} r_{1m} \\ r_{2m} \\ \dots \\ r_{Lm} \end{pmatrix} \quad (6)$$

4 性能分析

基于上述密钥生成算法,采用 MATLAB 编程对密钥生成速率进行模拟,分析方法的性能指标,如图 4 所示,在根密钥数量有限的情况下,分别采用两段方式、三段方式和四段方式组合生成大量的新鲜密钥,生成的密钥数量与根密钥呈类指数关系增加,同时随着分段数量的增加,密钥生成数量急剧增加,生成效率大幅提高,满足大量终端对密钥更新的需求。

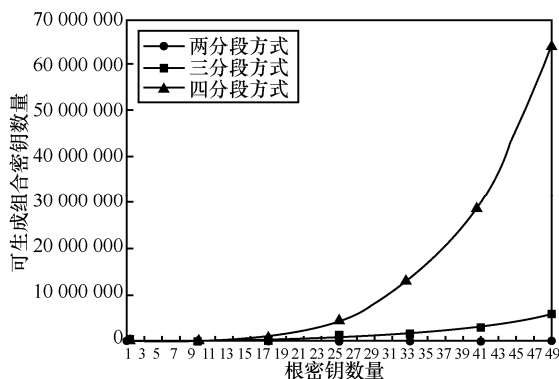


图4 不同分段条件下的密钥生成效率对比

以配用电终端为例,主站与台区量子密钥分

发速率为 10 kbit/s,每个台区下的终端数量不等,分别设置为 500、1 000、1 500 和 2 000,采用一次一密、对称加密的方式,对称密钥分组的密码采用 256 位密钥,根密钥更新速率为 39 次/s。采用常规量子密钥加密方式和本文的分片组合加密方式的密钥更新速率对比如图 5 所示,根据数据业务的重要性和传输速率设置不同的密钥更新速率,采用两段分片组合的情况下,500 台终端的密钥更新速率最高达到 60 次/s,满足要求;在 2 000 台终端的情况下,采用三段分片的方式,密钥更新速率达到 1 300 次/s。可见该方法提供了足够的量子组合密钥。

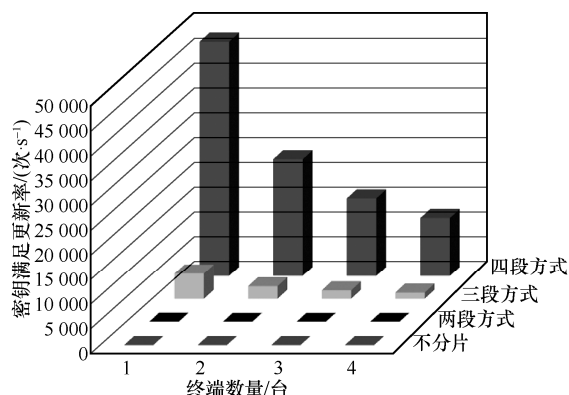


图5 不同终端数量和分段数情况下密钥的更新速率

5 结束语

针对配用电终端数量大、分布广的特点,提出一种基于组合密钥的密钥生成技术。该方案采用初始密钥作为种子密钥,以较少密钥组合大量相异的密钥,解决密钥有限和大量终端需求数量的问题,保障终端设备都能共享足够的安全密钥。由于采用了组合的思想来实现对称密钥的一次一变,具有良好的安全优势,可对种子密钥进行有效的保护。密钥因子矩阵经过组合产生大量的共享密钥,从而使得较小的存储空间可存储大量的密钥,有利于降低大量密钥所需的存储空间受限问题,具有应用简单、可扩展性好的特征,适用于点多面广的大规模配用电终端网络。



参考文献:

- [1] 国家电网公司. 国家电网公司“十三五”通信网规划[R]. 2016.
State Grid Corporation of China. The 13th five-year plan for communication network of state grid corporation[R]. 2016.
- [2] 汪来富, 金华敏, 刘东鑫, 等. 面向网络大数据的安全分析技术应用[J]. 电信科学, 2017, 33(3): 112-118.
WANG L F, JIN H M, LIU D X, et al. Application of security analysis technology for network big data[J]. Telecommunications Science, 2017, 33(3): 112-118.
- [3] 张东霞, 姚良忠, 马文媛. 中外智能电网发展战略[J]. 中国电机工程学报, 2013(31): 1-16.
ZHANG D X, YAO L Z, MA W Y. Development strategies of smart grid at home and abroad [J]. Chinese journal of electrical engineering, 2013(31): 1-16.
- [4] 吴昊. 基于业务的电力通信网安全风险评估方法研究[D]. 北京: 华北电力大学, 2015.
WU H. Research on security risk assessment method of power-communication network based on services[D]. Beijing: North China Electric Power University, 2015.
- [5] KUMAR V, HUSSAIN M. Secure communication for advance metering infrastructure in smart grid[C]// 2014 Annual IEEE India Conference, Dec 3-7, 2014, New Delhi, India. Piscataway: IEEE Press, 2014: 1-6.
- [6] 刘国荣, 刘东鑫, 汪来富, 等. 云端协同的智能终端数据加密技术[J]. 电信科学, 2018, 34(2): 111-114.
LIU G R, LIU D X, WANG L F, et al. Cloud collaborative intelligent terminal data encryption technology [J]. Telecommunications Science, 2018, 34(2): 111-114.
- [7] XIAO S, GONG W, TOWSLEY D. Secure wireless communication with dynamic secrets[C]// 2015 IEEE INFOCOM, April 26-May 1, 2015, San Francisco, CA, USA. Piscataway: IEEE Press, 2015: 1-9.
- [8] 潘涛. 数据安全及隐私保护在智能电网中的应用研究[J]. 通信技术, 2019, 52(4): 196-200.
PAN T. Data security and privacy protection in smart grid[J]. Communications Technology, 2019, 52(4): 196-200.
- [9] 刘振亚. 智能电网技术[M]. 北京: 中国电力出版社, 2010.
LIU Z Y. Smart grid technology [M]. Beijing: China Electric Power Press, 2010.
- [10] NICANFAR H, JOKAR P, BEZNOSOV K, et al. Efficient authentication and key management mechanisms for smart grid communications[J]. IEEE Systems Journal, 2014, 8(2): 629-640.

[作者简介]



高建 (1982-), 男, 北京智芯微电子科技有限公司高级工程师, 主要研究方向为电力系统自动化。



陈文彬 (1972-), 男, 北京智芯微电子科技有限公司高级工程师, 主要研究方向为信息通信。



庞建民 (1973-), 男, 北京智芯微电子科技有限公司工程师, 主要研究方向为通信技术及应用。