(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2019 年 7 月 18 日 (18.07.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/137014 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *H04L 9/08* (2006.01)

(21) 国际申请号: PCT/CN2018/102358

(22) 国际申请日: 2018 年 8 月 24 日 (24.08.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810025965.4 2018年1月11日 (11.01.2018) CN

(71) 申请人: 北京国电通网络技术有限公司(**BEIJING GUODIAN TONG NETWORK TECHNOLOGY CO., LTD**) [CN/CN]; 中国北京市丰台区航丰路1号时代财富天地大厦28层, Beijing 100070 (CN)。 华北电力大学(**NORTH CHINA ELECTRIC POWER UNIVERSITY**) [CN/CN]; 中国北京市昌平区回龙观镇北农路2号, Beijing 102206 (CN)。 国家电网有限公司(**STATE GRID CORPORATION OF CHINA**) [CN/CN]; 中国北京市西城区西长安街86号, Beijing 100031 (CN)。

(72) 发明人: 邓伟(**DENG, Wei**); 中国北京市丰台区航丰路1号时代财富天地大厦28层, Beijing 100070 (CN)。 吴文炤(**WU, Wenzhao**); 中国北京市丰台区航丰路1号时代财富天地大厦28层, Beijing 100070 (CN)。 于卓智(**YU, Zhuozhi**); 中国北京市丰台区航丰路1号时代财富天地大厦28层, Beijing 100070 (CN)。 张叶峰(**ZHANG, Yefeng**); 中国北京市丰台区航丰路1号时代财富天地大厦28层, Beijing 100070 (CN)。 韩冰洋(**HAN, Bingyang**); 中国北京市丰台区航丰路1号时代

(54) **Title:** QUANTUM KEY FUSION-BASED SECURE COMMUNICATION METHOD AND APPARATUS FOR VIRTUAL POWER PLANT, AND MEDIUM

(54) 发明名称: 基于量子密钥融合的虚拟电厂安全通信方法及装置、介质

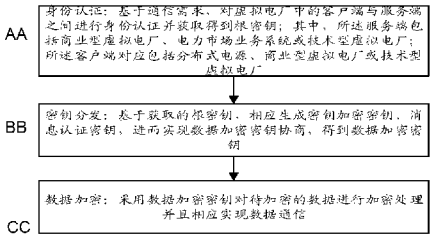

图 5

AA Identity authentication: on the basis of communication requirements, perform identity authentication between a client and a server in a virtual power plant and obtain a root key, wherein the server comprises a commercial virtual power plant, a power market service system or a technical virtual power plant, and the client correspondingly comprises a distributed power source, a commercial virtual power plant or a technical virtual power plant

BB Key distribution: on the basis of the obtained root key, correspondingly generate a key encryption key and a message authentication key, thereby implementing data encryption key negotiation to obtain a data encryption key

CC Data encryption: encrypt data to be encrypted using the data encryption key and correspondingly implement data communication

(57) **Abstract:** Disclosed are a quantum key fusion-based secure communication method for a virtual power plant, comprising: identity authentication: on the basis of communication requirements, performing identity authentication between a client and a server in a virtual power plant and obtaining a root key; key distribution: on the basis of the obtained root key, correspondingly generating a key encryption key and a message authentication key, thereby implementing data encryption key negotiation to obtain a data encryption key; and data encryption: encrypting data to be encrypted using the data encryption key and correspondingly implementing data communication. In the process of identity authentication or key distribution, a quantum key server is used to implement quantum key negotiation, and the negotiated quantum key is used to implement corresponding identity authentication or as a data encryption key. Also disclosed are a quantum key fusion-based secure communication apparatus for a virtual power plant and a computer storage medium.

(57) 摘要: 本申请公开了一种基于量子密钥融合的虚拟电厂安全通信方法，包括：身份认证：基于通信需求，对虚拟电厂中的客户端与服务端之间进行身份认证并获取得到根密钥；密钥分发：基于获取的根密钥，相应生成密钥加密密钥、消息认证密钥，进而实现数据加密密钥协商，得到数据加密密钥；数据加密：采用数据加密密钥对待加密的数据进行加密处理并且相应实现数据通信；上述进行身份认证或者密钥分发的过程中，利用量子密钥服务器实现量子密钥协商，并且将协商得到的量子密钥实现相应的身份认证或者作为数据加密密钥。本申请实施例还公开了一种基于量子密钥融合的虚拟电厂安全通信装置及计算机存储介质。

WO 2019/137014 A1

[见续页]

财富天地大厦28层, Beijing 100070 (CN)。 **冷曼(LENG, Man)**; 中国北京市丰台区航丰路1号时代财富天地大厦28层, Beijing 100070 (CN)。 **马永红(MA, Yonghong)**; 中国北京市昌平区回龙观镇北农路2号, Beijing 102206 (CN)。 **张京伦(ZHANG, Jinglun)**; 中国北京市昌平区回龙观镇北农路2号, Beijing 102206 (CN)。 **吴润泽(WU, Runze)**; 中国北京市昌平区回龙观镇北农路2号, Beijing 102206 (CN)。 **陈文伟(CHEN, Wenwei)**; 中国北京市丰台区航丰路1号时代财富天地大厦28层, Beijing 100070 (CN)。 **李楠翔(LI, Nanxiang)**; 中国北京市丰台区航丰路1号时代财富天地大厦28层, Beijing 100070 (CN)。 **朱玉坤(ZHU, Yukun)**; 中国北京市丰台区航丰路1号时代财富天地大厦28层, Beijing 100070 (CN)。

(74) 代理人: **北京派特恩知识产权代理有限公司(CHINA PAT INTELLECTUAL PROPERTY OFFICE)**; 中国北京市海淀区海淀南路21号中关村知识产权大厦B座2层, Beijing 100080 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

基于量子密钥融合的虚拟电厂安全通信方法及装置、介质

技术领域

本申请涉及电力技术领域但不限于电力技术领域，特别是指一种基于量子密钥融合的虚拟电厂安全通信方法及装置、计算机存储介质。

背景技术

当前，随着大量不同种类的新能源和分布式发电设备的并网发电，对电网调度和安全运行带来了新的严峻挑战。虚拟电厂是一种合理整合和优化利用分布式新能源的有效形式，同时也能有效参与电力市场的能源交易过程。但目前对于虚拟电厂的研究主要是从电力系统经济可靠运行的角度讨论问题，具体工作主要包括能源管理、系统运行、优化调度、预测建模等方面，而对如何依托先进密码、身份认证、加密通信等技术来保障信息通信安全，确保能源互联网的可靠运行尚未有高相关性内容的研究。

传统的信息安全措施基于数学问题的计算复杂性，在分布式计算、云计算和量子计算等数值计算能力日益发展的今天，传统密码学并不能保障数据传输的绝对安全，而量子密码学基于量子测不准原理，量子态测量塌缩和未知量子态不可克隆等物理定理，可以很好地保障信息传输的长期和绝对安全。近年来，虽然电力系统的信息安全受到人们的广泛关注，也有一些将量子密钥分配技术引入电力系统的研究。但纵观现有相关成果可以看出：现有工作要么单纯从量子密钥技术的角度进行讨论，要么只是简单的在电力系统中提出应用量子技术，成果与电力具体业务系统的结合深度不足，难以实现高效安全的通信手段，尤其是针对于虚拟电厂相关的通信安全。

发明内容

本申请的目的在于提出一种基于量子密钥融合的虚拟电厂安全通信方法及装置、计算机存储介质。

本申请实施例提供了一种基于量子密钥融合的虚拟电厂安全通信方法，包括:

身份认证：基于通信需求，对虚拟电厂中的客户端与服务端之间进行身份认证并获取得到根密钥；其中，所述服务端包括商业型虚拟电厂、电力市场业务系统或技术型虚拟电厂；所述客户端对应包括分布式电源、商业型虚拟电厂或技术型虚拟电厂；

密钥分发：基于获取的根密钥，相应生成密钥加密密钥、消息认证密钥，进而实现数据加密密钥协商，得到数据加密密钥；

数据加密：采用数据加密密钥对待加密的数据进行加密处理并且相应实现数据通信；

其中，上述进行身份认证或者密钥分发的过程中，利用量子密钥服务器实现量子密钥协商，并且将协商得到的量子密钥实现相应的身份认证或者作为数据加密密钥。

本申请实施例还提供一种基于量子密钥融合的虚拟电厂安全通信装置，包括:

身份认证模块，配置为身份认证：基于通信需求，对虚拟电厂中的客户端与服务端之间进行身份认证并获取得到根密钥；其中，所述服务端包括商业型虚拟电厂、电力市场业务系统或技术型虚拟电厂；所述客户端对应包括分布式电源、商业型虚拟电厂或技术型虚拟电厂；

分发模块，配置为密钥分发：基于获取的根密钥，相应生成密钥加密密钥、消息认证密钥，进而实现数据加密密钥协商，得到数据加密密钥；

加密模块，配置为数据加密：采用数据加密密钥对待加密的数据进行加密处理并且相应实现数据通信；

其中，上述进行身份认证或者密钥分发的过程中，利用量子密钥服务器实现量子密钥协商，并且将协商得到的量子密钥实现相应的身份认证或者作为数据加密密钥。

本申请实施例还提供一种计算机存储介质，所述计算机存储介质存储有计算机可执行指令；所述计算机可执行指令被执行后，能够实现前述的基于量子密钥融合的虚拟电厂安全通信方法。

本申请实施例提供的基于量子密钥融合的虚拟电厂安全通信方法，通过将量子密钥与经典加密方式进行融合的方式实现虚拟电厂的安全通信，即不会过多的增加成本，又能大大提高通信过程中的数据安全性。因此，本申请能够提供一种安全、可靠并且经济有效的安全通信方法，提高虚拟电厂通信安全性和可靠性。

附图说明

图 1 为本申请实施例提供的虚拟电厂通信网络结构示意图；

图 2 为本申请实施例提供的加密密钥与历史密钥哈希值关系示意图；

图 3 为本申请实施例提供的通过根密钥获得相关密钥的关系示意图；

图 4 为本申请实施例提供的虚拟电厂进行单播或者组播通信流程示意图；

图 5 为本申请实施例提供的基于量子密钥融合的虚拟电厂安全通信方法的流程示意图。

具体实施方式

为使本申请的目的、技术方案和优点更加清楚明白，以下结合具体实施例，并参照附图，对本申请进一步详细说明。

需要说明的是，本申请实施例中所有使用“第一”和“第二”的表述均是为了区分两个相同名称非相同的实体或者非相同的参量，可见“第一”“第二”仅为了表述的方便，不应理解为对本申请实施例的限定，后续实施例对此不再一一说明。

本申请针对于当前加密通信现状，考虑到量子产品的价格较高，可利用常用经典和量子密钥融合，进而提出了一种基于量子密钥融合的虚拟电厂安全通信方法，具有良好的应用前景。

为了更加清楚的理解本申请方案，首先对虚拟电厂相关信息作出解释，如下：虚拟电厂中的通信通常包含商业型虚拟电厂（CVPP）和分布式电源（DER）之间、CVPP和电力市场业务系统之间、CVPP和技术型虚拟电厂（TVPP）之间、TVPP 和 DER 之间的单播通信以及电力市场业务系统与CVPP之间的组播通信；参照图1所示，为本申请提供的虚拟电厂通信网络结构示意图。由图 1 可知，通常电力市场业务系统与多个商业型虚拟电厂（CVPP）以及传统电厂连接，而每个商业型虚拟电厂（CVPP）分别与不同的技术型虚拟电厂（TVPP）连接。其中，量子通信需要以下设备作为支撑：量子信道，用于量子信息的传输；量子可信中继设备，用于量子密钥的可信中继接力；量子密钥服务器，用于量子密钥的生成与管理；经典信道，用于传输量子密钥外的经典信息；量子随机数发生器，用于产生量子随机数作为密钥发送给量子密钥服务器和量子密钥管理装置，其隶属于量子密钥服务器；用户端量子密钥管理装置，用于产生相关的业务密钥。

在本申请一些实施例中，参照图 5 所示，所述基于量子密钥融合的虚拟电厂安全通信方法包括如下步骤：

（1）身份认证：基于通信需求，对虚拟电厂中的客户端与服务端之间进行身份认证并获取得到根密钥；其中，所述服务端包括商业型虚拟电厂、电力市场业务系统或技术型虚拟电厂；所述客户端对应包括分布式电源、商业型虚拟电厂或技术型虚拟电厂；例如：服务端为商业型虚拟电厂（CVPP），客户端为分布式电源（DER）。

在本申请一些实施例中，所述身份认证过程包括采用证书认证方式进行认证；其中，采用证书认证时需要可信的第三方分别给客户端和服务端签发相应证书；

采用证书认证过程包括如下步骤：

客户端将对应的身份信息 ID_C1、客户端证书，例如 X.509、客户端哈希值以及随机数 Nh 发送给相应的服务端；

服务端接收客户端发送的信息并且对信息进行验证，若验证信息符合，则给出根密钥，即授权密钥 AK，并且将根密钥利用证书中的公钥加密后发送给客户端；

客户端用对应的私钥解密得到同样的根密钥，完成身份认证。

在本申请另一些实施例中，所述身份认证过程包括采用快速认证方法进行认证；其中，客户端和服务端分别拥有历史数据索引表，所述历史数据索引表中包含时间、身份信息、各自的历史密钥与历史哈希值；客户端和服务端每次会话会产生加密密钥 k，记为 k_0，k_1，k_2……k_n，每次产生的历史密钥哈希值记为 h_1，h_2，h_3……h_n，将 k 的哈希值和 h 的哈希值进行异或运算，得到了新的历史密钥哈希值；参照图 2 所示，h_n 通过如下公式计算:

$$h_1 = SHA1[k_0] \oplus SHA1[k_1];$$

$$h_n = SHA1[h_{n-1}] \oplus SHA1[k_n];$$

其中，n 为大于 1 的自然数，SHA1 为哈希算法;

客户端和服务端根据历史数据索引表进行认证;

认证成功后授予根密钥。

在一些实施例中，所述客户端和服务端根据历史数据索引表进行认证的步骤还包括:

客户端在对应的历史数据索引表中提取得到索引表内的上次密钥值 k、上次时间 Ti 和索引值 ind;

客户端利用上次密钥值、上次时间和索引值计算哈希值，连带客户端的身份信息和随机数，作为报文发送给服务端；其中，该报文使用上次密钥值加密，并附上索引值;

所述报文表示为：$ESM4[SHA1(k|Ti|Ni|ind)|ID\_DER|Ni]_k|ind$;

其中，ESM4 为商密算法；k 为加密密钥；Ti 为上次时间；Ni 为随机数；ind 为索引值；ID_DER 为客户端的身份信息;

服务端接收到上述报文信息后，根据报文信息中的索引值检索服务端内的历史数据索引表并提取索引表中的相关信息，用加密密钥对报文信息进行解密，先对比解密得到的客户端身份信息以获取客户端的身份，然后利用索引表中对应的上次时间，加密密钥，索引值和随机数计算哈希值，与客户端发送的哈希值进行比对；若两者相等，则确认客户端的身份信息真实有效，接纳该客户端的认证，并更新历史数据索引表内的历史哈希值、历史密钥、时间相关信息；若哈希值不相等，则身份认证失败，中断通信；至此，服务端对于客户端的身份认证结束，认证成功后，随后进行根密钥

的生成，为密钥分发做准备。

服务端产生新的随机数 Nj，并将确认信息和新的时间 T 通过报文一起返回给客户端；报文用 k 加密，加密公式如下：$Encrypt(Nj|T)_k$;

客户端收到报文信息后进行解密，获得新随机数 Nj 和新时间 T;

服务端和客户端通过随机数 Ni、Nj、新时间 T 以及新历史哈希值 h 进行计算，得到新的根密钥 AK；其中，根密钥 AK 的计算公式为：

AK=Truncate_128[SHA1(Ni|Nj|T|h)]；其中，Truncate_128 表示取前 128 位。

这样，即使攻击方破解了密钥 k，但由于没有历史哈希值，所以也无法获得新的根密钥 AK。

在本申请一些实施例中，所述身份认证过程还可以利用量子密钥服务器实现量子密钥协商；其中，客户端和服务端均具有量子密钥服务器，客户端设置有量子密钥管理装置，在客户端和服务端进行通信之前，客户端的量子密钥管理装置预先在量子密钥服务器处进行绑定注册，量子密钥服务器要求量子随机数发生器产生大量随机数用作密钥存储在量子密钥服务器和客户端的量子密钥管理装置中；客户端的量子密钥管理装置与量子密钥服务器 L2 共享量子随机数密钥，服务端直接连接量子密钥服务器 L1;

利用量子密钥实现所述身份认证过程包括如下步骤:

客户端向服务端发送数据传输请求;

服务端收到请求后，产生随机数 Nb，并将所述随机数 Nb 与量子身份认证要求一起发送给客户端;

客户端收到量子身份认证要求后，通过客户端的量子密钥管理装置 QC 向绑定的量子密钥服务器 L2 发出服务信息，信息内容为服务端要求对客户端进行量子身份认证;

量子密钥服务器 L2 收到客户端的服务信息后，服务端的量子密钥服务器 L1 与客户端的量子密钥服务器 L2 进行量子密钥协商，量子密钥协商完成之后客户端和服务端得到达成一致的密钥 K_QU1;

服务端产生随机数作为根密钥 AK，计算信号 $E=AK\oplus K\_QU1$，并通过经典信道发送给量子密钥服务器 L2;

量子密钥服务器 L2 接收到信号 E 后，计算 $AK'=E\oplus K\_QU1$，并选择

客户端和量子密钥服务器L2之间预存的量子随机数Ni，计算ST=AK'⊕Ni；随后，量子密钥服务器L2将ST、随机数Ni指针ptr、长度long以及hash（AK'）一起发送给客户端；

客户端收到消息之后，使用随机数指针ptr及长度long提取随机数Ni，并计算AK''=ST⊕Ni，将消息摘要HMAC（AK''）$_{Nb}$发送给服务端；

服务端收到上述消息摘要后，计算HMAC（AK）$_{Nb}$是否与HMAC(AK'')$_{Nb}$一致，若一致，则确认客户端的身份，并使用AK作为根密钥；若不一致则认证失败，结束通信。

在一些实施例中，可采用无线通信设备收发数据，以应对客户端广分布所带来的通信布线困难问题。在无线通信情况下，客户端的量子密钥管理装置可通过定期到密钥管理服务器利用USB拷贝方式获得量子随机数。此后，可应用密钥对应用层数据加密，并可辅助采用802.16协议对低层数据加密。

（2）密钥分发：基于获取的根密钥，相应生成密钥加密密钥、消息认证密钥，进而实现数据加密密钥协商，得到数据加密密钥；参照图3所示，基于根密钥可以相应的衍生得到消息认证密钥、密钥加密密钥，进而利用密钥加密密钥得到业务加密密钥，也即数据加密密钥。

在本申请一些实施例中，所述密钥分发过程包括：

客户端向服务端发送密钥申请；其中，密钥申请中包含随机数Nh；

服务端接收到密钥申请后，根据根密钥Ak和随机数Nh生成密钥加密密钥KEK、上行消息认证密钥HMAC_key1及下行消息认证密钥HMAC_key2；所述密钥加密密钥KEK通过如下公式计算：

KEK=truncate_128{SHA1[(AK$\|$0^44)⊕Nh]}；其中，0^44表示44个0，Nh为64位随机数；

所述上行消息认证密钥通过如下公式计算：

HMAC_key1=truncate_160{SHA1[(AK$\|$$36^{44}$)⊕Nh]}；

所述下行消息认证密钥通过如下公式计算：

HMAC_key2=truncate_160{SHA1[(AK$\|$$36^{44}$)⊕Nh]}

其中，36^{44}表示对在128位根密钥AK后面连接44个0X36，形成352位比特串，然后对这480位比特串进行哈希运算，最后和随机数Nh进行异

或运算;

客户端和服务端进行数据加密密钥 TEK 的协商;其中,客户端向服务端发送协商申请,该申请消息使用 KEK 加密,消息摘要的密钥使用 HMAC_key1;

服务端收到请求后将 TEK 参数列表使用 KEK 加密并发送给客户端,发送消息摘要的密钥使用 HMAC_key2。

(3)数据加密:采用数据加密密钥对待加密的数据进行加密处理并且相应实现数据通信;其中,所述待加密的数据包括客户端发送给服务端的设备与运行状态参数、实时发电数据、边际成本、实时用电数据、储能容量和储能设备状态参数等。

在本申请一些实施例中,所述数据加密过程采用 SM4-CBC、DES、AES、SM1 中的一种或者多种组合算法对各应用层业务数据进行加密;其中,所有数据通过消息认证密钥进行哈希运算并附在数据尾部,且上行方向的哈希密钥采用上行消息认证密钥 HMAC_key1,下行方向的哈希密钥采用下行消息认证密钥 HMAC_key2。其中,CBC 是密码分组链接模式,目的是让重复的明文分组产生不同的密文分组。

由上述实施例可知,本申请提供的基于量子密钥融合的虚拟电厂安全通信方法,通过将量子密钥与经典加密方式进行融合的方式实现虚拟电厂的安全通信,即不会过多的增加成本,又能大大提高通信过程中的数据安全性。因此,本申请能够提供一种安全、可靠并且经济有效的安全通信方法,提高虚拟电厂通信安全性和可靠性。

在本申请一些实施例中,上述身份认证过程和密钥分发过程均利用量子密钥服务器实现量子密钥协商;

所述身份认证过程包括如下步骤:

客户端通过经典信道向服务端发送身份认证请求;

服务端收到身份认证请求后,通过量子随机数发生器产生一组随机数作为根密钥 AK,并要求量子密钥服务器 L2 和 L1 进行量子密钥协商;

量子密钥服务器 L1 和 L2 依据预定协议进行量子密钥协商后,得到密钥 K_QU2;

服务端获取密钥 K_QU2,计算 $E=AK\oplus K\_QU2$,并将 E 发送给客户端;

客户端计算 AK'=E⊕K_QU2 和 hash（AK'），并发送给服务端；

服务端判断 hash（AK'）是否等于 hash（AK），若相等，则完成了对于客户端的身份认证；若不等，则认证失败，中断通信；

所述密钥分发过程包括:

客户端和服务端以 AK 作为根密钥，产生对应的消息认证密钥和密钥加密密钥 KEK;

客户端要求量子密钥服务器 L1 和 L2 进行量子密钥协商；

量子密钥服务器 L1 和 L2 依据预定协议进行量子密钥协商，得到密钥 K_QU3;

客户端和服务端获得密钥 K_QU3，并将密钥 K_QU3 作为数据加密密钥。

最后按照同样的数据加密过程实现带加密数据的加密。

在一些实施例中，还可以在密钥分发过程采用量子一次一密方式进行双方安全通信，所述密钥分发过程包括:

客户端和服务端均以 AK 作为根密钥，然后衍生得到消息认证密钥;

客户端与服务端每次通信时，都要求量子密钥服务器 L1 和 L2 进行量子密钥协商;

量子密钥服务器 L1 和 L2 依据 BB84 协议进行量子密钥协商，得到密钥 K_QU4;

客户端和服务端获得 K_QU4，并将其作为数据加密密钥。

上述方式虽然对于量子密钥的消耗量较大，但可以保证数据的绝对安全。

在本申请一些实施例中，针对于组播情形，除了需要考虑上述通讯安全，而且需要考虑到新客户端的加入与退出引起的认证以及组密钥更新过程。首先，通常来说，组播主要包括电力市场各业务系统向各 CVPP 的组播信息，包括当前时段各种能源电价，未来时段能量需求等信息；还包括各种电力辅助市场需求信息，如一次调频、自动发电控制、调峰、无功调节、旋转备用、黑启动等业务信息。例如：设某电力市场业务系统包含 5 个 CVPP，该电力市场向 5 个客户端组播能量需求竞价方案消息，其中，组播中心为电力市场业务系统，组内客户端为各 CVPP。

因此基于本申请提出的方案，若通信为组播通信时，一个服务端对应多个客户端进行组播通信；参照图 4 所示，为本申请提供的虚拟电厂进行单播或者组播通信流程示意图。所述虚拟电厂通信方法还包括如下步骤：

1、组密钥初始化，实现过程如下：

初始化之前，各客户端首先在服务端处注册，并获得注册值；

各客户端向服务端发送注册值以及选择的随机数 B1~Bn；其中，n 为客户端的数量。Bn 为客户端 n 选择的随机数；

服务端收到随机数后，计算 B1*B2*…*Bn[G]作为组密钥；其中，G 为椭圆加密算法对应的基点；基于本方案使用椭圆加密算法实现，所使用的椭圆曲线为 E(a，b)，基点为 G(xG，yG)；

服务端向客户端发送组密钥时，将除当前客户端外其余客户端的随机数与基点乘积计算结果以及椭圆加密算法对应的椭圆曲线参数发给当前客户端，公式如下：Ci=B1*…*Bi-1*Bi+1*…*Bn[G]；其中，Ci 为当前第 i 个客户端对应的相关数据；

各客户端收到相关数据后，利用该相关数据与各自随机数计算得到组密钥；例如客户端 1 计算 C1*B1 作为组密钥。

这样，即使传输的密钥 Ci 被攻击，由于攻击者不具有客户端自身的随机数 Bi，因此，也无法获得组密钥。

2、新客户端认证：

当服务端中有新的客户端 M1 希望加入服务端 D1 的组播群组，且客户端已知组播加密所用的椭圆曲线、基点 G 以及服务端公钥 P；则新客户端获得组密钥的过程包括步骤：

新客户端计算 h(1)=SM3(Nm|ID_M1)，并向服务端发送加入组播群组的申请；其中，申请中包含随机数 Nm、新客户端 M1 的身份信息 ID_M1、新客户端的公钥 PM 和 h(1)；SM3 为哈希算法，且申请消息使用服务端公钥 P 加密，加密公式为：$SM2[Nm|ID\_M1|PM|h(1)]_p$；其中，SM2 为椭圆曲线加密算法；

服务端 D1 收到申请消息后，用私钥解密并向新客户端 M1 回复信息，要求新客户端 M1 发送身份证明材料；

新客户端 M1 收到服务端发送的消息后，若新客户端具有注册值，则向

服务端发送新客户端的注册值 KM1，并附带哈希值 h2=SM3(KM1)，若新客户端 M1 没有注册值，则向服务端发送证书 cert;

服务端 D1 首先根据哈希值 h2 进行消息认证，并验证该注册值或证书；若验证通过，则服务端 D1 生成密钥加密密钥 KEK，向新客户端 M1 发送使用新客户端的公钥 PM 加密的密钥加密密钥 KEK，并分配一个新的注册值 KM2；若验证不通过，则认证识别，中断通信；

服务端 D1 计算如下值:

T1=t1[G];

KE_down=T1+s*{hash(KM2)+hash(x)}[G];

X={s*hash(x)}[G]；其中，x 为正在使用的组密钥，t1 为当前时间，s 为服务端 D1 的私钥;

服务端 D1 计算哈希值 h(3)=SM3(KM2|T1|KE_down|X)，向新客户端 M1 发送 T1 和 X，并附上 h(3)用作消息认证;

新客户端 M1 接收消息 T1 和 X，利用已知的公钥 P 和其注册值 KM2，计算 KE_down'=T1+[hash(KM2)]P+X，并验证 hash(KM2|T1|KE_down'|X)是否与 h(3)相等；若验证通过，则新客户端 M1 生成 KE_up，并向服务端 D1 发送使用 KEK 加密的 KE_up，且附带哈希值 h(4)=SM3(KE_up)，服务端 D1 收到消息后，计算（KE_up*KE_down'）[G]作为新的组密钥；若验证失败，则中断通信;

这样，能够在不明显增加计算量的情况下实现了对服务端 D1 的身份认证，即实现了双向身份认证。

在本申请一些实施例中，所述新客户端认证过程还可以通过采用量子密钥协商的方式实现；其中，新客户端 M1 连接量子密钥服务器 L2；服务端连接量子密钥服务器 L1;

所述新客户端认证过程包括:

新客户端 M1 向服务端 D1 发起认证申请;

服务端 D1 收到认证申请消息后要求采用量子方式进行身份认证;

采用如上述实施例中同样的认证方式实现新客户端认证;

认证完成后，新客户端 M1 请求量子密钥服务器 L2 和 L1 依据预定协议进行量子密钥协商，得到量子密钥 K_QU5，双方计算（K_QU5*KE_down'）

[G]作为新的组密钥。这一方式一方面保证了 KE_up 的绝对安全，提高了组密钥的安全性，另外并不要求出新客户端 M1 之外的其他组内客户端拥有量子密钥服务器。

或者，

新客户端 M1 拥有量子密钥管理装置 QC，且量子密钥管理装置绑定量子密钥服务器 L2，QC 和 L2 拥有共享的量子随机数；服务端 D1 直接连接量子密钥服务器 L1；

所述新客户端认证过程包括：

新客户端 M1 向服务端 D1 发送认证申请；

服务端 D1 收到认证申请后，通过如上述实施例中同样的方式验证新客户端 M1 身份；

量子密钥服务器 L1 和 L2 进行量子密钥协商后得到量子密钥 K_QU6；

选择 QC 和 L2 之间预存的某段量子随机数为 Nc，L2 计算 E=Nc⊕K_QU6 并发送给新客户端 M1；

新客户端 M1 通过计算 E⊕Nc 得到 K_QU6，用 K_QU6 来加密 KE_up 进而实现身份认证。

3、组密钥更新：

对于以下两种情况，需要进行组密钥更新；

一、若有新加入客户端，新客户端的与服务端双向身份认证后，新客户端直接采用 K_group=(KE_up*KE_down)[G]作为新组播密钥；

对组内其它客户端，服务端 D1 将{KE_up，t1，SM3(KM1)}用原组播密钥加密，并附上哈希值 h(5)=SM3(KE_down)发给其它客户端，加密公式为：

$SM4[KE\_up|t1|SM3(KM1)]_x$；

组内其它客户端收到消息后，根据 KE_up，t1，SM3(KM1)，结合已知的 P 和 x，计算得到 KE_down”=t1[G]+[SM3(KM1)]P+SM3(x)P，验证 SM3(KE_down”) 是否与 h(5) 一致；若一致，则计算得到 K_group=(KE_up*KE_down”)[G]作为新的组播密钥；

二、若有客户端离开或者是密钥更新时间到，则服务端将选择的一个随机数 Nj 和其哈希值 SM3(Nj)发送给所有组内客户端，发送时用原组播密

钥加密数据;

组内客户端收到该消息后计算 K_group=Nj[G]+SM3(Nj)]P+SM3(x)P 作为新的组播密钥。

由上述实施例可知，本申请与现有技术相比，至少具有以下优点：1、针对虚拟电厂业务，提供考虑具体应用场景的安全通信方案。2、融合使用传统的经典密钥和无条件安全的量子密钥，保证虚拟电厂安全通信方案的可行性和逐步演进。3、针对虚拟电厂业务的单播和组播通信，提供了一整套包括全经典和量子融合安全通信方案。

本实施例还提供一种基于量子密钥融合的虚拟电厂安全通信装置，包括:

身份认证模块，配置为身份认证：基于通信需求，对虚拟电厂中的客户端与服务端之间进行身份认证并获取得到根密钥；其中，所述服务端包括商业型虚拟电厂、电力市场业务系统或技术型虚拟电厂；所述客户端对应包括分布式电源、商业型虚拟电厂或技术型虚拟电厂;

分发模块，配置为密钥分发：基于获取的根密钥，相应生成密钥加密密钥、消息认证密钥，进而实现数据加密密钥协商，得到数据加密密钥;

加密模块，配置为数据加密：采用数据加密密钥对待加密的数据进行加密处理并且相应实现数据通信;

其中，上述进行身份认证或者密钥分发的过程中，利用量子密钥服务器实现量子密钥协商，并且将协商得到的量子密钥实现相应的身份认证或者作为数据加密密钥。

在一些实施例中，所述认证模块，配置为客户端将对应的身份信息、客户端证书、客户端哈希值以及随机数发送给相应的服务端;

所述装置还包括:

接收模块，配置为服务端接收客户端发送的信息并且对信息进行验证，若验证信息符合，则给出根密钥，并且将根密钥利用证书中的公钥加密后发送给客户端;

所述认证模块，还配置为客户端用对应的私钥解密得到同样的根密钥，完成身份认证。

在一些实施例中，所述身份认证过程包括采用快速认证方法进行认证;

其中，客户端和服务端分别拥有历史数据索引表，所述历史数据索引表中包含时间、身份信息、各自的历史密钥与历史哈希值；客户端和服务端每次会话会产生密钥 k，记为 k_0，k_1，k_2……k_n，每次产生的历史密钥哈希值记为 h_1，h_2，h_3……h_n，将 k 的哈希值和 h 的哈希值进行异或运算，得到了新的历史密钥哈希值；h_n 通过如下公式计算：

$$h_1 = SHA1[k_0] \oplus SHA1[k_1];$$

$$h_n = SHA1[h_{n-1}] \oplus SHA1[k_n];$$

其中，n 为大于 1 的自然数，SHA1 为哈希算法；

客户端和服务端根据历史数据索引表进行认证；

认证成功后授予根密钥。

在一些实施例中，所述认证模块，还配置为客户端在对应的历史数据索引表中提取得到索引表内的上次密钥值 k、上次时间 Ti 和索引值 ind；

客户端利用上次密钥值、上次时间和索引值计算哈希值，连带客户端的身份信息和随机数，作为报文发送给服务端；其中，该报文使用上次密钥值加密，并附上索引值；所述报文表示为：$ESM4[SHA1(k|Ti|Ni|ind)|ID\_DER|Ni]_k|ind$；其中，ESM4 为商密算法；k 为加密密钥；Ti 为上次时间；Ni 为随机数；ind 为索引值；ID_DER 为客户端的身份信息；

服务端接收到上述报文信息后，根据报文信息中的索引值检索服务端内的历史数据索引表并提取索引表中的相关信息，用加密密钥对报文信息进行解密，先对比解密得到的客户端身份信息以获取客户端的身份，然后利用索引表中对应的上次时间，加密密钥，索引值和随机数计算哈希值，与客户端发送的哈希值进行比对；若两者相等，则确认客户端的身份信息真实有效，接纳该客户端的认证，并更新历史数据索引表内的历史哈希值、历史密钥、时间相关信息；若哈希值不相等，则身份认证失败，中断通信；

服务端产生新的随机数 Nj，并将确认信息和新的时间 T 通过报文一起返回给客户端；报文用 k 加密，加密公式如下：$Encrypt(Nj|T)_k$；

客户端收到报文信息后进行解密，获得新随机数 Nj 和新时间 T；

服务端和客户端通过随机数 Ni、Nj、新时间 T 以及新历史哈希值 h 进行计算，得到新的根密钥 AK；其中根密钥 AK 的计算公式为：

AK=Truncate_128[SHA1(Ni|Nj|T|h)]；其中，Truncate_128 表示取前 128 位。

在一些实施例中，所述分发模块，还配置为客户端向服务端发送密钥申请；其中，密钥申请中包含随机数 Nh;

服务端接收到密钥申请后，根据根密钥 Ak 和随机数 Nh 生成密钥加密密钥 KEK、上行消息认证密钥 HMAC_key1 及下行消息认证密钥 HMAC_key2；所述密钥加密密钥 KEK 通过如下公式计算:

KEK=truncate_128{SHA1[(AK | 0^44) ⊕ Nh]}；其中，0^44 表示 44 个 0，Nh 为 64 位随机数;

所述上行消息认证密钥通过如下公式计算:

HMAC_key1=truncate_160{SHA1[(AK | 36^{44}) ⊕ Nh]};

所述下行消息认证密钥通过如下公式计算:

HMAC_key2=truncate_160{SHA1[(AK | 36^{44}) ⊕ Nh]}

36^{44} 表示对在 128 位根密钥 AK 后面连接 44 个 0X36，形成 352 位比特串，然后对这 480 位比特串进行哈希运算，最后和随机数 Nh 进行异或运算;

客户端和服务端进行数据加密密钥 TEK 的协商；其中客户端向服务端发送协商申请，该申请消息使用 KEK 加密，消息摘要的密钥使用 HMAC_key1;

服务端收到请求后将 TEK 参数列表使用 KEK 加密并发送给客户端，发送消息摘要的密钥使用 HMAC_key2。

在一些实施例中，所述数据加密过程采用 SM4-CBC、DES、AES、SM1 中的一种或者多种组合算法对各应用层业务数据进行加密；其中，所有数据通过消息认证密钥进行哈希运算并附在数据尾部，且上行方向的哈希密钥采用上行消息认证密钥 HMAC_key1，下行方向的哈希密钥采用下行消息认证密钥 HMAC_key2。

在还有一些实施例中，所述身份认证过程利用量子密钥服务器实现量子密钥协商；其中，客户端和服务端均具有量子密钥服务器，客户端设置有量子密钥管理装置，在客户端和服务端进行通信之前，客户端的量子密钥管理装置预先在量子密钥服务器处进行绑定注册，量子密钥服务器要求量子随机数发生器产生大量随机数用作密钥存储在量子密钥服务器和客户

端的量子密钥管理装置中；客户端的量子密钥管理装置与量子密钥服务器L2共享量子随机数密钥，服务端直接连接量子密钥服务器L1；

所述认证模块，配置为客户端向服务端发送数据传输请求；

服务端收到请求后，产生随机数Nb，并将所述随机数Nb与量子身份认证要求一起发送给客户端；

客户端收到量子身份认证要求后，通过客户端的量子密钥管理装置QC向绑定的量子密钥服务器L2发出服务信息，信息内容为服务端要求对客户端进行量子身份认证；

量子密钥服务器L2收到客户端的服务信息后，服务端的量子密钥服务器L1与客户端的量子密钥服务器L2进行量子密钥协商，量子密钥协商完成之后客户端和服务端得到达成一致的密钥K_QU1；

服务端产生随机数作为根密钥AK，计算信号E=AK⊕K_QU1，并通过经典信道发送给量子密钥服务器L2；

量子密钥服务器L2接收到信号E后，计算AK'=E⊕K_QU1，并选择客户端和量子密钥服务器L2之间预存的量子随机数Ni，计算ST=AK'⊕Ni；随后，量子密钥服务器L2将ST、随机数Ni指针ptr、长度long以及hash（AK'）一起发送给客户端；

客户端收到消息之后，使用随机数指针ptr及长度long提取随机数Ni，并计算AK''=ST⊕Ni，将消息摘要HMAC（AK''）$_{Nb}$发送给服务端；

服务端收到上述消息摘要后，计算HMAC（AK）$_{Nb}$是否与HMAC(AK'')$_{Nb}$一致，若一致，则确认客户端的身份，并使用AK作为根密钥；若不一致则认证失败，结束通信。

在一些实施例中，所述身份认证过程和密钥分发过程均利用量子密钥服务器实现量子密钥协商；

所述认证模块，还配置为客户端通过经典信道向服务端发送身份认证请求；服务端收到身份认证请求后，通过量子随机数发生器产生一组随机数作为根密钥AK，并要求量子密钥服务器L2和L1进行量子密钥协商；量子密钥服务器L1和L2依据预定协议进行量子密钥协商后，得到密钥K_QU2；服务端获取密钥K_QU2，计算E=AK⊕K_QU2，并将E发送给客户端；客户端计算AK'=E⊕K_QU2和hash（AK'），并发送给服务端；服

务端判断 hash（AK'）是否等于 hash（AK），若相等，则完成了对于客户端的身份认证；若不等，则认证失败，中断通信；

所述分发模块，配置为客户端和服务端以 AK 作为根密钥，产生对应的消息认证密钥和密钥加密密钥 KEK；客户端要求量子密钥服务器 L1 和 L2 进行量子密钥协商；量子密钥服务器 L1 和 L2 依据预定协议进行量子密钥协商，得到密钥 K_QU3；客户端和服务端获得密钥 K_QU3，并将密钥 K_QU3 作为数据加密密钥。

在一些实施例中，若通信为组播通信时，一个服务端对应多个客户端进行组播通信；

该装置还包括：

组密钥初始模块，配置为各客户端首先在服务端处注册，并获得注册值；

各客户端向服务端发送注册值以及选择的随机数 B1~Bn；

服务端收到随机数后，计算 B1*B2*…*Bn[G]作为组密钥；其中，G 为椭圆加密算法对应的基点；

服务端向客户端发送组密钥时，将除当前客户端外其余客户端的随机数与基点乘积计算结果以及椭圆加密算法对应的椭圆曲线参数发给当前客户端，公式如下：Ci=B1*…*Bi-1*Bi+1*…*Bn[G]；其中，Ci 为当前第 i 个客户端对应的相关数据；

各客户端收到相关数据后，利用该相关数据与各自随机数计算得到组密钥；

所述认证模块，还配置为新客户端认证：当服务端中有新的客户端希望加入服务端的组播群组，且客户端已知组播加密所用的椭圆曲线、基点 G 以及服务端公钥 P；则新客户端获得组密钥的过程包括步骤：新客户端计算 h(1)=SM3(Nm|ID_M1)，并向服务端发送加入组播群组的申请；其中，申请中包含随机数 Nm、新客户端 M1 的身份信息 ID_M1、新客户端的公钥 PM 和 h(1)；SM3 为哈希算法，且申请消息使用服务端公钥 P 加密，加密公式为：$SM2[Nm|ID\_M1|PM|h(1)]_p$；其中，SM2 为椭圆曲线加密算法；

服务端 D1 收到申请消息后，用私钥解密并向新客户端 M1 回复信息，要求新客户端 M1 发送身份证明材料；新客户端 M1 收到服务端发送的消息

后，若新客户端具有注册值，则向服务端发送新客户端的注册值 KM1，并附带哈希值 h2=SM3(KM1)，若新客户端 M1 没有注册值，则向服务端发送证书 cert；服务端 D1 首先根据哈希值 h2 进行消息认证，并验证该注册值或证书；若验证通过，则服务端 D1 生成密钥加密密钥 KEK，向新客户端 M1 发送使用新客户端的公钥 PM 加密的密钥加密密钥 KEK，并分配一个新的注册值 KM2；若验证不通过，则认证识别，中断通信；

服务端 D1 计算如下值：

T1=t1[G];

KE_down=T1+s*{hash(KM2)+hash(x)}[G];

X={s*hash(x)}[G]；其中，x 为正在使用的组密钥，t1 为当前时间，s 为服务端 D1 的私钥；

服务端 D1 计算哈希值 h(3)=SM3(KM2|T1|KE_down|X)，向新客户端 M1 发送 T1 和 X，并附上 h(3)用作消息认证；

新客户端 M1 接收消息 T1 和 X，利用已知的公钥 P 和其注册值 KM2，计算 KE_down'=T1+[hash(KM2)]P+X，并验证 hash(KM2|T1|KE_down'|X)是否与 h(3)相等；若验证通过，则新客户端 M1 生成 KE_up，并向服务端 D1 发送使用 KEK 加密的 KE_up，且附带哈希值 h(4)=SM3(KE_up)，服务端 D1 收到消息后，计算（KE_up*KE_down'）[G]作为新的组密钥；若验证失败，则中断通信；

组密钥更新：

对于以下两种情况，需要进行组密钥更新；

一、若有新加入客户端，新客户端的与服务端双向身份认证后，新客户端直接采用 K_group=(KE_up*KE_down)[G]作为新组播密钥；

对组内其它客户端，服务端 D1 将{KE_up，t1，SM3(KM1)}用原组播密钥加密，并附上哈希值 h(5)=SM3(KE_down)发给其它客户端，加密公式为：

$SM4[KE\_up|t1|SM3(KM1)]_x$;

组内其它客户端收到消息后，根据 KE_up，t1，SM3(KM1)，结合已知的 P 和 x，计算得到 KE_down''=t1[G]+[SM3(KM1)]P+SM3(x)P，验证 SM3(KE_down'') 是否与 h(5) 一致；若一致，则计算得到

K_group=(KE_up*KE_down'')[G]作为新的组播密钥;

二、若有客户端离开或者是密钥更新时间到，则服务端将选择的一个随机数 Nj 和其哈希值 SM3(Nj)发送给所有组内客户端，发送时用原组播密钥加密数据;

组内客户端收到该消息后计算 K_group=Nj[G]+SM3(Nj)]P+SM3(x)P 作为新的组播密钥。

在一些实施例中，所述新客户端认证过程还可以通过采用量子密钥协商的方式实现；其中，新客户端 M1 连接量子密钥服务器 L2；服务端连接量子密钥服务器 L1;

所述认证模块，配置为新客户端认证，可包括:

新客户端 M1 向服务端 D1 发起认证申请;

服务端 D1 收到认证申请消息后要求采用量子方式进行身份认证;

采用如权利要求 9 中同样的认证方式实现新客户端认证;

认证完成后，新客户端 M1 请求量子密钥服务器 L2 和 L1 依据预定协议进行量子密钥协商,得到量子密钥 K_QU5,双方计算(K_QU5*KE_down')[G]作为新的组密钥;

或者,

新客户端 M1 拥有量子密钥管理装置 QC，且量子密钥管理装置绑定量子密钥服务器 L2，QC 和 L2 拥有共享的量子随机数；服务端 D1 直接连接量子密钥服务器 L1;

所述新客户端认证过程包括:

新客户端 M1 向服务端 D1 发送认证申请;

服务端 D1 收到认证申请后，通过如权利要求 9 中方式验证新客户端 M1 身份;

量子密钥服务器 L1 和 L2 进行量子密钥协商后得到量子密钥 K_QU6;

选择 QC 和 L2 之间预存的某段量子随机数为 Nc，L2 计算 E=Nc⊕K_QU6 并发送给新客户端 M1;

新客户端 M1 通过计算 E⊕Nc 得到 K_QU6，用 K_QU6 来加密 KE_up 进而实现身份认证。

本发明实施例还提供一种计算机存储介质，所述计算机存储介质存储

有计算机可执行指令；所述计算机可执行指令被执行后，能够实现前述一个或多个实施例提供的基于量子密钥融合的虚拟电厂安全通信方法；例如，如图 3 和/或图 4 所示的方法。

所属领域的普通技术人员应当理解：以上任何实施例的讨论仅为示例性的，并非旨在暗示本公开的范围（包括权利要求）被限于这些例子；在本申请的思路下，以上实施例或者不同实施例中的技术特征之间也可以进行组合，步骤可以以任意顺序实现，并存在如上所述的本申请的不同方面的许多其它变化，为了简明它们没有在细节中提供。

本申请的实施例旨在涵盖落入所附权利要求的宽泛范围之内的所有这样的替换、修改和变型。因此，凡在本申请的精神和原则之内，所做的任何省略、修改、等同替换、改进等，均应包含在本申请的保护范围之内。

权利要求书

1. 一种基于量子密钥融合的虚拟电厂安全通信方法，包括:

身份认证：基于通信需求，对虚拟电厂中的客户端与服务端之间进行身份认证并获取得到根密钥；其中，所述服务端包括商业型虚拟电厂、电力市场业务系统或技术型虚拟电厂；所述客户端对应包括分布式电源、商业型虚拟电厂或技术型虚拟电厂；

密钥分发：基于获取的根密钥，相应生成密钥加密密钥、消息认证密钥，进而实现数据加密密钥协商，得到数据加密密钥；

数据加密：采用数据加密密钥对待加密的数据进行加密处理并且相应实现数据通信；

其中，上述进行身份认证或者密钥分发的过程中，利用量子密钥服务器实现量子密钥协商，并且将协商得到的量子密钥实现相应的身份认证或者作为数据加密密钥。

2. 根据权利要求 1 所述的方法，其中，所述身份认证过程包括采用证书认证方式进行认证；其中，采用证书认证时需要可信的第三方分别给客户端和服务端签发相应证书；

认证过程包括:

客户端将对应的身份信息、客户端证书、客户端哈希值以及随机数发送给相应的服务端；

服务端接收客户端发送的信息并且对信息进行验证，若验证信息符合，则给出根密钥，并且将根密钥利用证书中的公钥加密后发送给客户端；

客户端用对应的私钥解密得到同样的根密钥，完成身份认证。

3. 根据权利要求 1 所述的方法，其中，所述身份认证过程包括采用快速认证方法进行认证；其中，客户端和服务端分别拥有历史数据索引表，所述历史数据索引表中包含时间、身份信息、各自的历史密钥与历史哈希值；客户端和服务端每次会话会产生密钥 k，记为 k_0，k_1，k_2……k_n，每次产生的历史密钥哈希值记为 h_1，h_2，h_3……h_n，将 k 的哈希值和 h 的哈希值进行异或运算，得到了新的历史密钥哈希值；h_n 通过如下公式计算:

$$h_1 = SHA1[k_0] \oplus SHA1[k_1];$$

$h_n = SHA1[h_{n-1}] \oplus SHA1[k_n]$;

其中，n 为大于 1 的自然数，SHA1 为哈希算法；

客户端和服务端根据历史数据索引表进行认证；

认证成功后授予根密钥。

4. 根据权利要求 3 所述的方法，其中，所述客户端和服务端根据历史数据索引表进行认证的步骤还包括：

客户端在对应的历史数据索引表中提取得到索引表内的上次密钥值 k、上次时间 Ti 和索引值 ind；

客户端利用上次密钥值、上次时间和索引值计算哈希值，连带客户端的身份信息和随机数，作为报文发送给服务端；其中，该报文使用上次密钥值加密，并附上索引值；所述报文表示为：$ESM4[SHA1(k|Ti|Ni|ind)|ID\_DER|Ni]_k|ind$；其中，ESM4 为商密算法；k 为加密密钥；Ti 为上次时间；Ni 为随机数；ind 为索引值；ID_DER 为客户端的身份信息；

服务端接收到上述报文信息后，根据报文信息中的索引值检索服务端内的历史数据索引表并提取索引表中的相关信息，用加密密钥对报文信息进行解密，先对比解密得到的客户端身份信息以获取客户端的身份，然后利用索引表中对应的上次时间，加密密钥，索引值和随机数计算哈希值，与客户端发送的哈希值进行比对；若两者相等，则确认客户端的身份信息真实有效，接纳该客户端的认证，并更新历史数据索引表内的历史哈希值、历史密钥、时间相关信息；若哈希值不相等，则身份认证失败，中断通信；

服务端产生新的随机数 Nj，并将确认信息和新的时间 T 通过报文一起返回给客户端；报文用 k 加密，加密公式如下：$Encrypt(Nj|T)_k$；

客户端收到报文信息后进行解密，获得新随机数 Nj 和新时间 T；

服务端和客户端通过随机数 Ni、Nj、新时间 T 以及新历史哈希值 h 进行计算，得到新的根密钥 AK；其中根密钥 AK 的计算公式为：

AK=Truncate_128[SHA1(Ni|Nj|T|h)]；其中，Truncate_128 表示取前 128 位。

5. 根据权利要求 1 所述的方法，其中，所述密钥分发过程包括：

客户端向服务端发送密钥申请；其中，密钥申请中包含随机数 Nh；

服务端接收到密钥申请后，根据根密钥 Ak 和随机数 Nh 生成密钥加密密钥 KEK、上行消息认证密钥 HMAC_key1 及下行消息认证密钥 HMAC_key2；所述密钥加密密钥 KEK 通过如下公式计算:

KEK=truncate_128{SHA1[(AK | 0^44)⊕Nh]}；其中，0^44 表示 44 个 0，Nh 为 64 位随机数;

所述上行消息认证密钥通过如下公式计算:

HMAC_key1=truncate_160{SHA1[(AK | 36^{44})⊕Nh]};

所述下行消息认证密钥通过如下公式计算:

HMAC_key2=truncate_160{SHA1[(AK | 36^{44})⊕Nh]}

36^{44} 表示对在 128 位根密钥 AK 后面连接 44 个 0X36，形成 352 位比特串，然后对这 480 位比特串进行哈希运算，最后和随机数 Nh 进行异或运算;

客户端和服务端进行数据加密密钥 TEK 的协商；其中客户端向服务端发送协商申请，该申请消息使用 KEK 加密，消息摘要的密钥使用 HMAC_key1;

服务端收到请求后将 TEK 参数列表使用 KEK 加密并发送给客户端，发送消息摘要的密钥使用 HMAC_key2。

6. 根据权利要求 1 所述的方法，其中，所述数据加密过程采用 SM4-CBC、DES、AES、SM1 中的一种或者多种组合算法对各应用层业务数据进行加密；其中，所有数据通过消息认证密钥进行哈希运算并附在数据尾部，且上行方向的哈希密钥采用上行消息认证密钥 HMAC_key1，下行方向的哈希密钥采用下行消息认证密钥 HMAC_key2。

7. 根据权利要求 1 所述的方法，其中，所述身份认证过程利用量子密钥服务器实现量子密钥协商；其中，客户端和服务端均具有量子密钥服务器，客户端设置有量子密钥管理装置，在客户端和服务端进行通信之前，客户端的量子密钥管理装置预先在量子密钥服务器处进行绑定注册，量子密钥服务器要求量子随机数发生器产生大量随机数用作密钥存储在量子密钥服务器和客户端的量子密钥管理装置中；客户端的量子密钥管理装置与量子密钥服务器 L2 共享量子随机数密钥，服务端直接连接量子密钥服务器 L1;

所述身份认证过程包括:

客户端向服务端发送数据传输请求;

服务端收到请求后，产生随机数 Nb，并将所述随机数 Nb 与量子身份认证要求一起发送给客户端;

客户端收到量子身份认证要求后，通过客户端的量子密钥管理装置 QC 向绑定的量子密钥服务器 L2 发出服务信息，信息内容为服务端要求对客户端进行量子身份认证;

量子密钥服务器 L2 收到客户端的服务信息后，服务端的量子密钥服务器 L1 与客户端的量子密钥服务器 L2 进行量子密钥协商，量子密钥协商完成之后客户端和服务端得到达成一致的密钥 K_QU1;

服务端产生随机数作为根密钥 AK，计算信号 E=AK⊕K_QU1，并通过经典信道发送给量子密钥服务器 L2;

量子密钥服务器 L2 接收到信号 E 后，计算 AK'=E⊕K_QU1，并选择客户端和量子密钥服务器 L2 之间预存的量子随机数 Ni，计算 ST=AK'⊕Ni;随后，量子密钥服务器 L2 将 ST、随机数 Ni 指针 ptr、长度 long 以及 hash（AK'）一起发送给客户端;

客户端收到消息之后，使用随机数指针 ptr 及长度 long 提取随机数 Ni，并计算 AK''=ST⊕Ni，将消息摘要 $HMAC(AK'')_{Nb}$ 发送给服务端;

服务端收到上述消息摘要后，计算 $HMAC(AK)_{Nb}$ 是否与 $HMAC(AK'')_{Nb}$ 一致，若一致，则确认客户端的身份，并使用 AK 作为根密钥;若不一致则认证失败，结束通信。

8. 根据权利要求 1 所述的方法，其中，所述身份认证过程和密钥分发过程均利用量子密钥服务器实现量子密钥协商;

所述身份认证过程包括:

客户端通过经典信道向服务端发送身份认证请求;

服务端收到身份认证请求后，通过量子随机数发生器产生一组随机数作为根密钥 AK，并要求量子密钥服务器 L2 和 L1 进行量子密钥协商;

量子密钥服务器 L1 和 L2 依据预定协议进行量子密钥协商后，得到密钥 K_QU2;

服务端获取密钥 K_QU2，计算 E=AK⊕K_QU2，并将 E 发送给客户端;

客户端计算 AK'=E⊕K_QU2 和 hash（AK'），并发送给服务端;

服务端判断 hash（AK'）是否等于 hash（AK），若相等，则完成了对于客户端的身份认证；若不等，则认证失败，中断通信；

所述密钥分发过程包括：

客户端和服务端以 AK 作为根密钥，产生对应的消息认证密钥和密钥加密密钥 KEK；

客户端要求量子密钥服务器 L1 和 L2 进行量子密钥协商；

量子密钥服务器 L1 和 L2 依据预定协议进行量子密钥协商，得到密钥 K_QU3；

客户端和服务端获得密钥 K_QU3，并将密钥 K_QU3 作为数据加密密钥。

9. 根据权利要求 1 所述的方法，其中，若通信为组播通信时，一个服务端对应多个客户端进行组播通信；

该方法还包括：

组密钥初始化，包括：

各客户端首先在服务端处注册，并获得注册值；

各客户端向服务端发送注册值以及选择的随机数 B1~Bn；

服务端收到随机数后，计算 B1*B2*…*Bn[G]作为组密钥；其中，G 为椭圆加密算法对应的基点；

服务端向客户端发送组密钥时，将除当前客户端外其余客户端的随机数与基点乘积计算结果以及椭圆加密算法对应的椭圆曲线参数发给当前客户端，公式如下：Ci=B1*…*Bi-1*Bi+1*…*Bn[G]；其中，Ci 为当前第 i 个客户端对应的相关数据；

各客户端收到相关数据后，利用该相关数据与各自随机数计算得到组密钥；

新客户端认证：

当服务端中有新的客户端希望加入服务端的组播群组，且客户端已知组播加密所用的椭圆曲线、基点 G 以及服务端公钥 P；则新客户端获得组密钥的过程包括步骤：

新客户端计算 h(1)=SM3(NmlID_M1)，并向服务端发送加入组播群组的申请；其中，申请中包含随机数 Nm、新客户端 M1 的身份信息 ID_M1、新

客户端的公钥 PM 和 h(1)；SM3 为哈希算法，且申请消息使用服务端公钥 P 加密，加密公式为：$SM2[Nm|ID\_M1|PM|h(1)]_p$；其中，SM2 为椭圆曲线加密算法；

服务端 D1 收到申请消息后，用私钥解密并向新客户端 M1 回复信息，要求新客户端 M1 发送身份证明材料；

新客户端 M1 收到服务端发送的消息后，若新客户端具有注册值，则向服务端发送新客户端的注册值 KM1，并附带哈希值 h2=SM3(KM1)，若新客户端 M1 没有注册值，则向服务端发送证书 cert；

服务端 D1 首先根据哈希值 h2 进行消息认证，并验证该注册值或证书；若验证通过，则服务端 D1 生成密钥加密密钥 KEK，向新客户端 M1 发送使用新客户端的公钥 PM 加密的密钥加密密钥 KEK，并分配一个新的注册值 KM2；若验证不通过，则认证识别，中断通信；

服务端 D1 计算如下值：

T1=t1[G]；

KE_down=T1+s*{hash(KM2)+hash(x)}[G]；

X={s*hash(x)}[G]；其中，x 为正在使用的组密钥，t1 为当前时间，s 为服务端 D1 的私钥；

服务端 D1 计算哈希值 h(3)=SM3(KM2|T1|KE_down|X)，向新客户端 M1 发送 T1 和 X，并附上 h(3)用作消息认证；

新客户端 M1 接收消息 T1 和 X，利用已知的公钥 P 和其注册值 KM2，计算 KE_down'=T1+[hash(KM2)]P+X，并验证 hash(KM2|T1|KE_down'|X)是否与 h(3)相等；若验证通过，则新客户端 M1 生成 KE_up，并向服务端 D1 发送使用 KEK 加密的 KE_up，且附带哈希值 h(4)=SM3(KE_up)，服务端 D1 收到消息后，计算（KE_up*KE_down'）[G]作为新的组密钥；若验证失败，则中断通信；

组密钥更新：

对于以下两种情况，需要进行组密钥更新；

一、若有新加入客户端，新客户端的与服务端双向身份认证后，新客户端直接采用 K_group=(KE_up*KE_down)[G]作为新组播密钥；

对组内其它客户端，服务端 D1 将{KE_up，t1，SM3(KM1)}用原组播

密钥加密，并附上哈希值 h(5)=SM3(KE_down)发给其它客户端，加密公式为:

$SM4[KE\_up|t1|SM3(KM1)]_x$;

组内其它客户端收到消息后，根据 KE_up，t1，SM3(KM1)，结合已知的 P 和 x，计算得到 KE_down”=t1[G]+[SM3(KM1)]P+SM3(x)P，验证 SM3(KE_down”) 是否与 h(5) 一致；若一致，则计算得到 K_group=(KE_up*KE_down”)[G]作为新的组播密钥;

二、若有客户端离开或者是密钥更新时间到，则服务端将选择的一个随机数 Nj 和其哈希值 SM3(Nj)发送给所有组内客户端，发送时用原组播密钥加密数据;

组内客户端收到该消息后计算 K_group=Nj[G]+SM3(Nj)]P+SM3(x)P 作为新的组播密钥。

10. 根据权利要求 9 所述的方法，其中，所述新客户端认证过程还可以通过采用量子密钥协商的方式实现；其中，新客户端 M1 连接量子密钥服务器 L2；服务端连接量子密钥服务器 L1;

所述新客户端认证过程包括:

新客户端 M1 向服务端 D1 发起认证申请;

服务端 D1 收到认证申请消息后要求采用量子方式进行身份认证;

采用如权利要求 9 中同样的认证方式实现新客户端认证;

认证完成后，新客户端 M1 请求量子密钥服务器 L2 和 L1 依据预定协议进行量子密钥协商，得到量子密钥 K_QU5，双方计算(K_QU5*KE_down’)[G]作为新的组密钥;

或者，

新客户端 M1 拥有量子密钥管理装置 QC，且量子密钥管理装置绑定量子密钥服务器 L2，QC 和 L2 拥有共享的量子随机数；服务端 D1 直接连接量子密钥服务器 L1;

所述新客户端认证过程包括:

新客户端 M1 向服务端 D1 发送认证申请;

服务端 D1 收到认证申请后，通过如权利要求 9 中方式验证新客户端 M1 身份;

量子密钥服务器 L1 和 L2 进行量子密钥协商后得到量子密钥 K_QU6;

选择 QC 和 L2 之间预存的某段量子随机数为 Nc，L2 计算 E=Nc⊕K_QU6 并发送给新客户端 M1;

新客户端 M1 通过计算 E⊕Nc 得到 K_QU6，用 K_QU6 来加密 KE_up 进而实现身份认证。

11、一种基于量子密钥融合的虚拟电厂安全通信装置，包括:

身份认证模块，配置为身份认证：基于通信需求，对虚拟电厂中的客户端与服务端之间进行身份认证并获取得到根密钥；其中，所述服务端包括商业型虚拟电厂、电力市场业务系统或技术型虚拟电厂；所述客户端对应包括分布式电源、商业型虚拟电厂或技术型虚拟电厂;

分发模块，配置为密钥分发：基于获取的根密钥，相应生成密钥加密密钥、消息认证密钥，进而实现数据加密密钥协商，得到数据加密密钥;

加密模块，配置为数据加密：采用数据加密密钥对待加密的数据进行加密处理并且相应实现数据通信;

其中，上述进行身份认证或者密钥分发的过程中，利用量子密钥服务器实现量子密钥协商，并且将协商得到的量子密钥实现相应的身份认证或者作为数据加密密钥。

12. 根据权利要求 11 所述的装置，其中，

所述认证模块，配置为客户端将对应的身份信息、客户端证书、客户端哈希值以及随机数发送给相应的服务端;

所述装置还包括:

接收模块，用于服务端接收客户端发送的信息并且对信息进行验证，若验证信息符合，则给出根密钥，并且将根密钥利用证书中的公钥加密后发送给客户端;

所述认证模块，还用于客户端用对应的私钥解密得到同样的根密钥，完成身份认证。

13、一种计算机存储介质，所述计算机存储介质存储有计算机可执行指令；所述计算机可执行指令被执行后，能够实现权利要求 1 至 10 任一项提供的基于量子密钥融合的虚拟电厂安全通信方法。

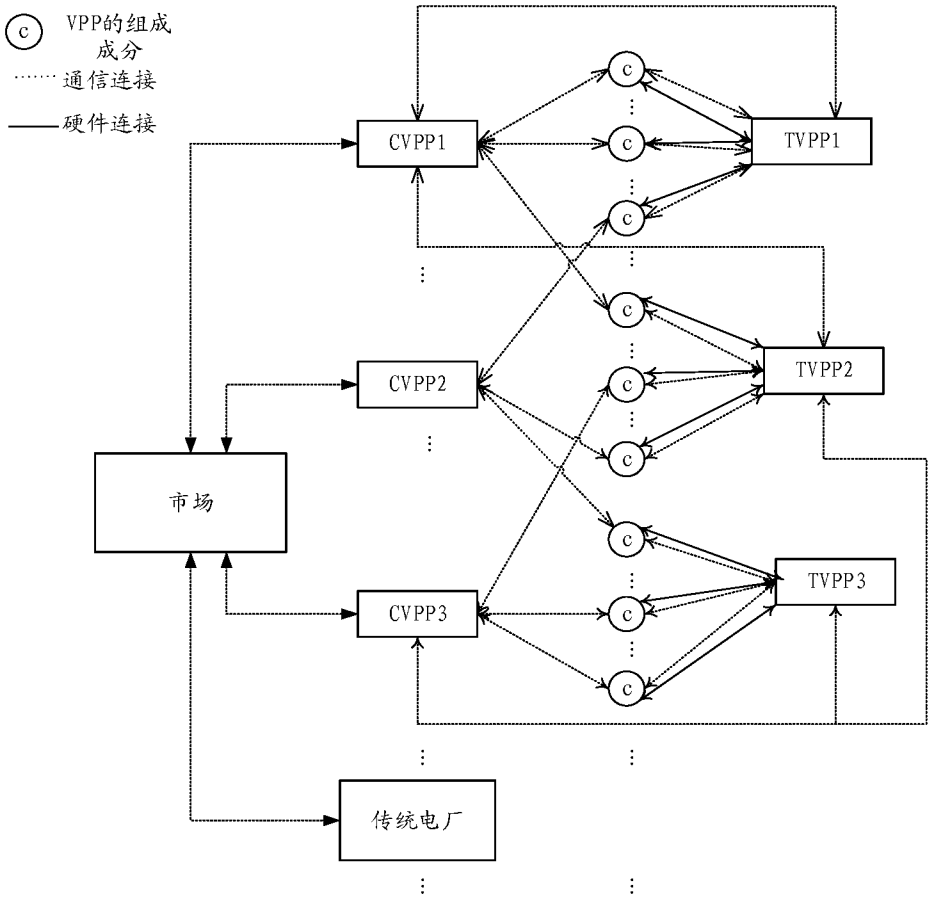
C VPP的组成成分
通信连接
硬件连接
CVPP1
CVPP2
CVPP3
TVPP1
TVPP2
TVPP3
市场
传统电厂

图 1

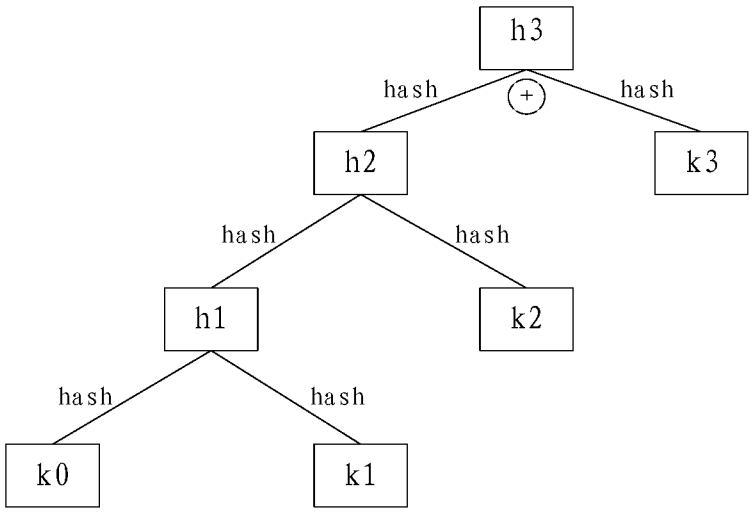
h3
hash
+
hash
h2
k3
hash
hash
h1
k2
hash
hash
k0
k1

图 2

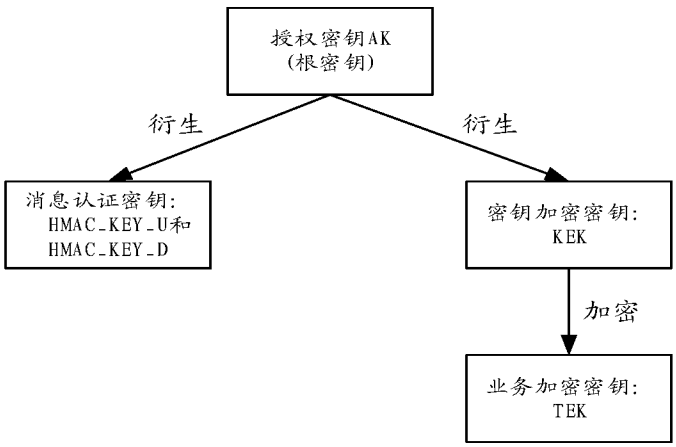
授权密钥AK
(根密钥)
衍生
衍生
消息认证密钥:
HMAC_KEY_U和
HMAC_KEY_D
密钥加密密钥:
KEK
加密
业务加密密钥:
TEK

图 3

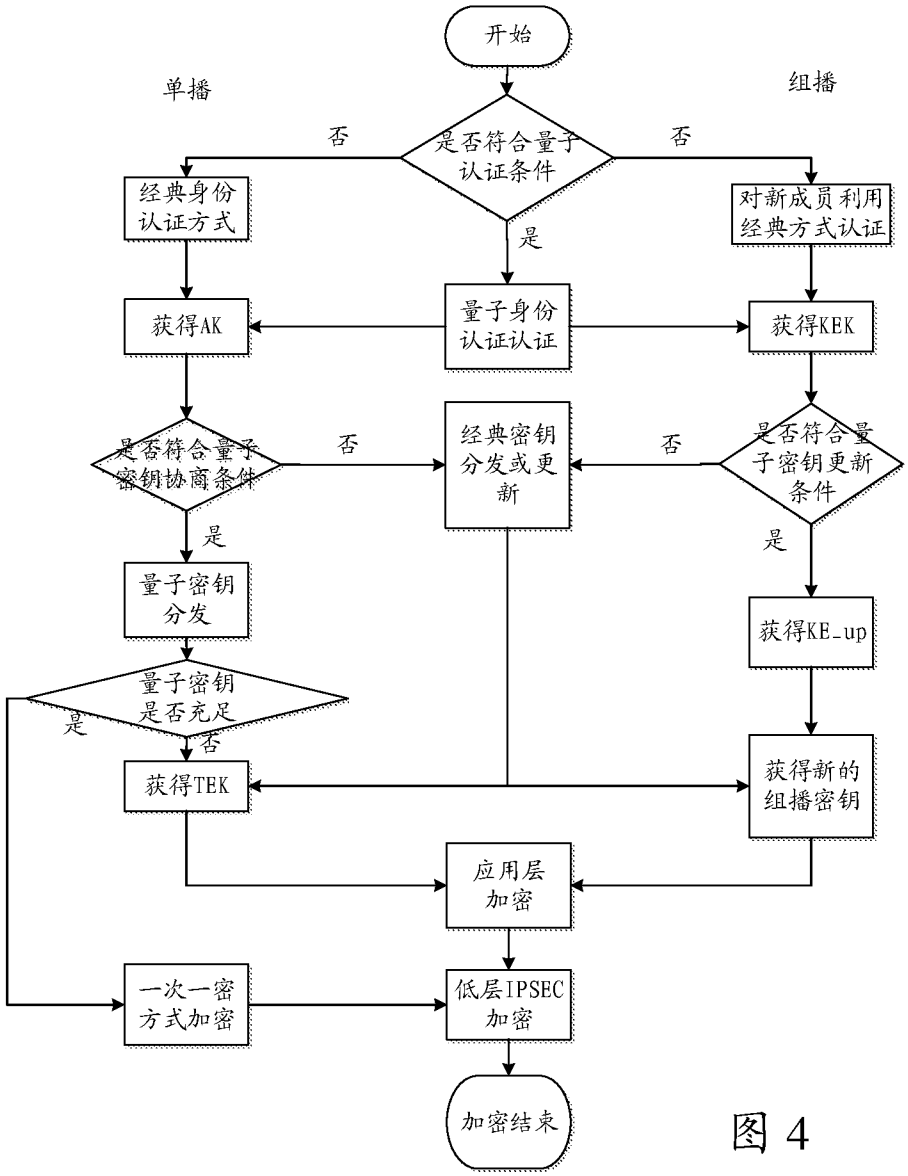
开始
单播
组播
是否符合量子认证条件
否
否
是
经典身份认证方式
对新成员利用经典方式认证
获得AK
量子身份认证认证
获得KEK
是否符合量子密钥协商条件
否
经典密钥分发或更新
否
是否符合量子密钥更新条件
是
是
量子密钥分发
获得KE_up
量子密钥是否充足
是
否
获得TEK
获得新的组播密钥
应用层加密
一次一密方式加密
低层IPSEC加密
加密结束

图 4

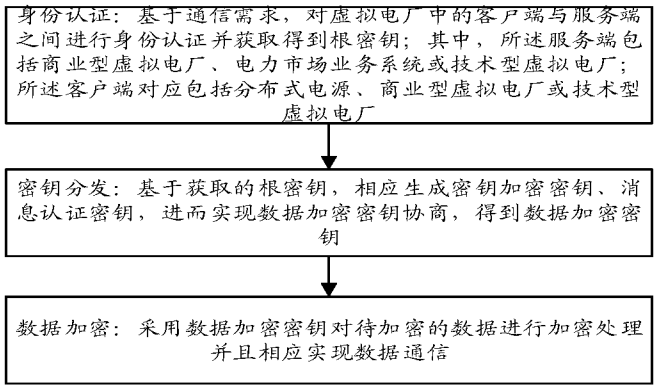
身份认证：基于通信需求，对虚拟电厂中的客户端与服务端之间进行身份认证并获取得到根密钥；其中，所述服务端包括商业型虚拟电厂、电力市场业务系统或技术型虚拟电厂；所述客户端对应包括分布式电源、商业型虚拟电厂或技术型虚拟电厂
密钥分发：基于获取的根密钥，相应生成密钥加密密钥、消息认证密钥，进而实现数据加密密钥协商，得到数据加密密钥
数据加密：采用数据加密密钥对待加密的数据进行加密处理并且相应实现数据通信

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/102358

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 9/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS; CNKI; CNTXT; USTXT; WOTXT; EPTXT; VEN: 量子密钥, 虚拟电厂, 电网, 协商, 加密, 密钥, 根密钥, 数据, 身份验证, 认证; quantum key, virtual power plant, power grid, negotiation, encrypt, key, root key, authentication, verification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 108234501 A (BEIJING GUODIANTONG NETWORK TECHNOLOGY CO., LTD. ET AL.) 29 June 2018 (2018-06-29) claims 1-10, and description, paragraphs 111-231	1-13
A	李治 (LI, Zhi). "电力系统信息安全关键技术的研究 (The Research of Key Technique on the Network Security for Power System)" *中国优秀博硕士学位论文全文数据库(硕士)工程科技II辑 (Non-official translation: Science-Engineering (B), Chinese Selected Doctoral Dissertations and Master's Theses Full-Text Databases (Master)), no. 4, 2004,* 15 December 2004 (2004-12-15), entire document	1-13
A	方燕琼等 (FANG, Yanqiong et al.). "虚拟电厂研究综述 (A Review on Virtual Power Plant)" *供用电 (Distribution & Utilization), no. 04, 2016,* 30 April 2016 (2016-04-30), entire document	1-13
A	SHABANZADEH, M. et al. ""An Interactive Cooperation Model for Neighboring Virtual Power Plant"" *Applied Energy 200(2017),* 18 May 2017 (2017-05-18), entire document	1-13
A	CN 107480847 A (ZHENGZHOU UNIVERSITY) 15 December 2017 (2017-12-15) entire document	1-13

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 October 2018	**29 October 2018**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing** **100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/102358

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 108234501 A	29 June 2018	None	
CN 107480847 A	15 December 2017	None	

国际检索报告

国际申请号
PCT/CN2018/102358

A. 主题的分类

H04L 29/06(2006.01)i; H04L 9/08(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CPRSABS;CNKI;CNTXT;USTXT;WOTXT;EPTXT;VEN:量子密钥，虚拟电厂,电网，协商,加密,密钥,根密钥，数据,身份验证,认证; quantum key, virtual power plant, power grid, negotiation, encrypt, key, root key, authentication, verification

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 108234501 A (北京国电通网络技术有限公司等) 2018年 6月 29日 (2018-06-29) 权利要求1-10，说明书第111-231段	1-13
A	李治. ""电力系统信息安全关键技术的研究"" 《中国优秀博硕士学位论文全文数据库（硕士）工程科技II辑》，2004年第04期, 2004年 12月 15日 (2004-12-15), 全文	1-13
A	方燕琼等. ""虚拟电厂研究综述"" 《供用电》，2016年第04期, 2016年 4月 30日 (2016-04-30), 全文	1-13
A	M. Shabanzadeh等. ""An interactive cooperation model for neighboring virtual power plant"" 《Applied Energy 200(2017)》，2017年 5月 18日 (2017-05-18), 全文	1-13
A	CN 107480847 A (郑州大学) 2017年 12月 15日 (2017-12-15) 全文	1-13

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2018年 10月 8日	2018年 10月 29日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 郑杰 电话号码 86-(010)-62412014

表 PCT/ISA/210 (第2页) (2015年1月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/102358

检索报告引用的专利文件	公布日（年/月/日）	同族专利	公布日（年/月/日）
CN 108234501 A	2018年 6月 29日	无	
CN 107480847 A	2017年 12月 15日	无	