

[身份认证]

基于量子密钥分配的电力计量终端双向身份认证

文/呼日查 刘敏 弓昊 鲁虎雄 杜国伟 李雪峰
内蒙古电力（集团）有限责任公司电能计量分公司

身份认证是电力计量终端安全通信的基础，同时也是通信过程中必不可少的环节，但现行认证方法在实际应用中效果并不理想，不仅认证速率比较慢，而且伪造身份通过比例比较高，严重威胁到电力计量终端通信安全。为此，提出基于量子密钥分配的电力计量终端双向身份认证研究。设计电力计量终端双向身份认证应用场景，基于场景下利用量子密钥分配技术实现终端与主站双方密钥协商，利用协商的密钥对电力计量终端双向身份初始认证，利用双方共享比特串对双向身份二次认证，实现基于量子密钥分配的电力计量终端双向身份认证。经实验证明，设计方法认证速率可以达到22组/s，伪造身份通过比例不超过0.1%，身份认证效果良好。

智能电网是信息化与工业化深度融合的产物，它通过先进的传感测量技术、通信技术、信息技术和自动控制技术等，实现对电网的实时监控、优化调度和高效管理。电力计量终端作为智能电网的重要组成部分，其安全性和可靠性直接关系到电网的稳定运行和用户的用电安全。然而，随着网络技术的不断发展，电力计量终端面临着来自网络空间的各种攻击，如身份伪造、数据篡改和恶意控制等，这些攻击不仅导致电力计量数据的失真，还对电网的稳定运行造成严重影响。电力计量终端作为智能电网的重要组成部分，需要实现与主站系统之间的双向身份认证。一方面，电力计量终端需要验证主站系统的身份和权限，确保接收到的指令和数据合法性；另一方面，主站系统也需要验证电力计量终端的身份和状态，确保采集到的数据的真实性和准确性。因此，研究基于量子密钥分配的电力计量终端双向身份认证机制，对于保障智能电网的安全稳定运行具有重要意义。

文献[1]提出基于椭圆曲线的认证方法，结合椭圆

圆曲线的数学特性和公钥密码学的思想，为通信双方提供一种身份认证机制。文献[2]提出基于共识算法的身份认证方法，通过引入共识算法的思想，实现对通信网络中节点的安全接入和可靠传输。传统的身份认证和密钥分配机制主要依赖于计算复杂性，即利用数学难题的求解难度来保证通信的安全性，为此提出基于量子密钥分配的电力计量终端双向身份认证研究。

电力计量终端双向身份认证应用场景设计

对于电力计量终端双向身份认证应用场景，假设一个由主站TP（即信任方）和一系列用户（电力计量终端）共同构成认证体系。这个体系的核心在于所有成员共同持有一个高度机密的 n 位二进制字符串 g ，这个密钥的存在成为界定组织成员身份的关键标识。在这个星型架构的组织中，当电力计量终端与TP之间需要通信时，终端首先向TP发出请求，随后TP会负责建立并连接两个用户之间的量子通信信道。电力计量终端向TP发送一个请求，请求

与主站建立通信。在接收到这一请求后，TP会迅速响应，并建立起电力计量终端和主站之间的量子通信信道。电力计量终端和主站会进行一系列的身份认证。首先，进行窃听检测，以确保通信信道未被第三方非法监听。一旦确认信道安全，电力计量终端会对主站进行身份认证，以确认其身份的真实性。这一步骤通过对比主站持有的密钥中的特定部分来实现，只有持有正确密钥的用户才能通过认证。

在成功认证终端的身份后，会再次进行窃听检测和身份认证。这一次，是由主站对终端进行身份认证。这种双向的认证机制极大地提高了通信的安全性，因为即使一方被攻陷，另一方也能通过认证机制发现异常。在双方的身份认证过程中，终端和主站持有的密钥是通过量子密钥分配产生的。去除掉用于窃听检测的粒子，因为这些粒子在密钥分发过程中已经不再需要。剩下的粒子则会被视为密钥分发的关键组成部分，它们将被用于终端与主站持有密钥共享。

基于量子密钥分配的终端双方密钥协商

基于以上设计的应用场景，利用量子密钥分配进行电力计量终端与主站之间的密钥协商，生成电力计量终端与主站的密钥。在密钥协商过程中，TP制备一个光子量子态序列，这个序列被标记为 P_1 。在这个序列 P_1 中，每个光子并不是处于单一的量子态，而是随机地处于线偏振基或圆偏振基中的某一个量子态，总共有四个可能的态，这种随机性的引入是为了增强通信的安全性。这些量子态在物理上是非正交的，这就意味着它们之间不能同时被精确地测量。这一特性对于防止窃听者进行非法操作至关重要。如果非法方试图对量子态进行窃听测量并转发，由于量子态的非正交性，这种操作必然会引入错误，这些错误会被通信双方（终端和主站）发现，从而确保通信的安全性。TP对终端和主站的随机身份信息比特串进行处理，将这个比特串通过一个量子单向函数进行处理，得到一个新的属于终端和主站的量子态序列，该两个态序列作为各自持有的密钥。将光子量子态序列中任意三个量子态作为量子单向函数的输入，对输入量子态进行Hadamard变换，用公式表示为

$$x = (Ha)(c - S)(e + ID)m_1m_2m_3 \quad (1)$$

式中， x 为Hadamard变换的量子态； H 为Hadamard

变换因子； a 为量子状态参数； c 为初始量子态； S 为交换操作； e 为随机数；ID为终端或主站的身份信息比特串； m_1 、 m_2 、 m_3 分别为输入的三个量子态。

通过对量子态变换后得到粒子的混合态为新的量子态序列。经过这样的处理，只要没有冒充者伪造身份信息比特串，那么无论是对终端还是主站，计算得到的量子态序列都将是相同的。这种一致性是验证通信双方身份和通信内容真实性的关键，任何对量子态的篡改或伪造都会导致量子态序列的不一致性，从而被通信双方所察觉。通过以上分析得到电力计量终端与主站的密钥，用于后续双向身份认证。

电力计量终端双向身份认证

在完成密钥协商后，TP将电力计量终端持有密钥与主站持有的密钥进行比较。如果双方的密钥值相等，则可以推断出没有非法方试图伪造身份信息与终端进行通信，此时通信可以安全地继续进行。如果双方的密钥值不相等，则可以推断出非法方试图伪造身份信息与终端进行通信，中断通信。以上过程用公式表示为

$$E = \begin{cases} 0, x_e = x_i \\ 1, x_e \neq x_i \end{cases} \quad (2)$$

式中， E 为电力计量终端双向身份初始认证结果；0为继续认证；1为终止通信； x_e 、 x_i 分别为电力计量终端和主站持有的密钥。

仅仅通过比较 x_e 与 x_i 并不能完全排除非法方的存在。因为一旦非法方截获了 x_e 与 x_i ，就有可能冒充合法身份。为进一步提高身份认证的可靠性，需要一个最终认证阶段。在确认身份无误后，终端会向TP发送一个继续认证的消息“continue”以及他的量子态序列，这一步骤用公式表示为

$$S(\text{contine}, x_e) \rightarrow TP \quad (3)$$

式中， S 为电力计量终端身份ID。

TP记录终端量子态序列中选择错误的测量基，将其标记为 N ，得到一个测量基错误信息序列。TP根据这个错误信息序列制备出一串纠错光子量子态序列，用公式表示为

$$H = \{N_1, N_2, \dots, N_i\} \quad (4)$$

式中， H 为纠错光子量子态序列； N_i 为第 i 个纠错光子量子态。

TP将纠错光子量子态序列和测量基错误信息序

列发送给终端，终端根据测量基错误信息序列更正测量基选择错误的位置，并测量校正后的量子态数列。这样，终端就可以对一系列的光子态进行完整地判断，并记录下来。当不受非法因素的影响时，被测得的量子状态和原始的量子态应当是完全相同的。在这一点上，终端与主站共用同一比特串序列，而终端将比特串序列比较的信息发送给主站。

终端和主站会向第三方公开一部分共享的比特串，第三方会对比共享的比特串的内容，如果两者相等，那么第三方会发送一个消息给终端，确认主站的身份是真实的；如果两者不相等，那么第三方将宣布通信失败，认证不成功，这表明可能有非法方介入了通信过程，通过以上方法实现基于量子密钥分配的电力计量终端双向身份认证。

实验论证

1. 实验设计与指标筛选

为验证本文设计的双向身份认证方法的性能，以某配电网为实验对象，该配电网中电力计量终端数量为80台，型号为HUIFA-A4F5，利用本文设计方法对该配电网内电力计量终端通信中双向身份进行认证。为全面检验方法的性能，本次实验以电力计量终端双向身份认证速率和伪造身份通过比例作为评价指标，身份认证速率会影响到电力计量终端通信速率，实验以电力计量终端数量为变量，统计不同终端数量下电力计量终端双向身份认证速率。

伪造身份通过比例可以反映出身份认证准确性和有效性，以电力计量终端通信并发数作为变量，统计在终端双向身份认证中伪造身份通过认证的比例，比例越高，则说明身份认证准确性越低。

2. 实验结果与讨论

实验将本文方法与文献[1]方法和文献[2]方法对比，表1、表2给出了三种方法身份认证速率和伪造身份通过比例，对比三种方法性能。

从表1中数据可以看出，设计方法电力计量终端双向身份认证速率平均为22组/s，相比较文献[1]方法和文献[2]方法，认证速率处于比较高的水平。从表2中数据可以看出，设计方法伪造身份通过比例不超过0.1%，而文献[1]方法通过比例在10%以上，文献[2]方法通过比例在15%以上，远远高于设计方法。通过以上对比证明，设计方法在电力计量终端

双向身份认证方面具有绝对的优势，可以实现对电力计量终端双向身份的准确认证。

表1 电力计量终端双向身份认证速率

(单位：组/s)

电力计量终端数量/台	本文方法	文献[1]方法	文献[2]方法
10	21	8	11
20	22	9	12
30	23	8	12
40	22	8	14
50	24	7	16
60	21	8	15
70	25	9	12
80	22	7	11

表2 伪造身份通过比例

(%)

并发数/条	本文方法	文献[1]方法	文献[2]方法
100	0.01	10.22	15.26
200	0.02	11.25	16.35
300	0.01	11.35	16.47
400	0.02	11.54	16.85
500	0.03	11.62	16.96
600	0.02	11.85	16.99
700	0.04	11.75	16.75
800	0.05	11.68	16.85

结束语

本文深入探讨基于量子密钥分配的电力计量终端双向身份认证机制，这一机制为电力计量终端的安全接入和数据传输提供强有力的保障。通过本研究，展示量子密钥分配技术在电力计量终端身份认证中的应用潜力。量子密钥分配以其无条件的安全性和实时性，为电力计量终端提供前所未有的安全保障。同时，双向身份认证机制的设计确保通信双方的身份真实性和数据完整性，有效防范身份伪造和数据篡改等安全威胁。EA

(收稿日期：2024-05-28)

参考文献

[1] 张心艺，宋建涛，杜杨．一种基于椭圆曲线的物联网双向身份认证协议[J]．软件导刊，2020，19(10)：233-237.

[2] 翟迪，张东磊，安春燕，等．基于共识算法的换流站无线传感网安全接入身份认证机制[J]．电力信息与通信技术，2024，22(4)：63-69.