IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 11, 2018, accepted January 8, 2019, date of publication January 21, 2019, date of current version April 2, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2893056

Lightweight Quantum Encryption for Secure Transmission of Power Data in Smart Grid

YUANCHENG LI[1], PAN ZHANG[1, 2], AND RONG HUANG[1]

[1]School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China
[2]State Grid Information and Telecommunication Branch, Beijing 100761, China

Corresponding author: Rong Huang (st_hr_mail@163.com)

This work was supported by the Fundamental Research Funds for the Central Universities under Grant 2018ZD06.

ABSTRACT The rise of the smart grid, which applies the Internet and smart metering technologies to the power system, results in massive, heterogeneous power data and a large number of attacks on the smart grid and causes great threats to the confidentiality and integrity of the power data. At the same time, with the development of quantum information, it is possible to use quantum cryptography to protect data transmission. Aiming at the problem of data security transmission in smart grid, this paper proposes a lightweight transmission scheme for power data security. In the scheme, we combine quantum cryptography with "one-time pad" mechanism, use a quantum random number generator which compensates the defects of the traditional random number generator and quantum key distribution protocol which ensure the security of key distribution, and design a new lightweight stream cipher encryption algorithm. Through theoretical analysis and experiments, it is proved that the proposed transmission scheme can ensure the security of power data transmission.

INDEX TERMS Authentication, one-time pad, power data, quantum cryptography, random number generator.

I. INTRODUCTION

As an Emerging Technology, the smart grid which combined with the advanced information communication technology (ICT) provides an effective means for integrating various renewable energy sources into existing power systems, and realizes a reliable, safe, economic, efficient and environmentally friendly power system. Intelligent communications technologies and information processing technologies have penetrated all aspects of power energy systems, such as generation, transmission, distribution, and home appliances [1], [2]. The widespread use of advanced information and communication technologies, particularly smart metering technology, generates vast amounts of electricity data. On the one hand, these data bring great benefits to better energy planning, more efficient energy generation and distribution. On the other hand, these can increase the stability and reliability of the smart grid. However, these technologies have also brought new security problems. Due to the coexistence of traditional SCADA with advanced metering infrastructure (AMI) and information technology (IT) systems, the interoperation of the data needs to call application programming interface (API), thus exposing the grid to cyber-attacks, such as meta-data spoofing, wrapping, Dos and phishing [3]. These attacks would affect the stability of the operation of the power system and may even cause widespread power outages, leading huge losses to the national economy and adversely influence to the social environment. Hence, a new technology is urgently needed to ensure the security of data transmission in the smart grid.

To ensure the security of communication in power system, the relevant security organizations considered the security requirements and traffic restrictions, recommended the cryptographic algorithms widely used in the IT network, and introduced a series of user guides and security standards, such as IEC 62351, ANSI/ISA-99.02. 01- 2009, AGA-12, to guide the companies to utilize encryption and authentication to ensure the communication security of power system [4], [5]. AGA-12 and IEC 62351 used RSA, elliptic curve (ECC) [6] or other classical asymmetric encryption algorithms to protect the power data. However, the speed of these algorithms was limited by the performance of power system and the power data increases exponentially, they did not meet the high real-time. To handle the problem which traditional TCP/IP-based network infrastructure didn't meet Industrial Internet of things (IIoTs), Premnath *et al.* [7] used the lightweight NTRU encryption to ensure the integrity and confidentiality of power data in the SCADA system. However, NTRU did not provide a complete system of decryption, there has

some legal cipher text cannot be decrypted, so it wasn't suitable for power system. Although lightweight encryption algorithm achieved low power consumption and hardware costs, to some extent they affected the performance of the power system. In addition, key management, including key generation and distribution, is important for the security of data transmission in smart grids [8]–[10]. Tsai and Lo [8] utilize an identity-based signature scheme and an identity-based encryption scheme to propose a new anonymous key distribution scheme for smart grid. Odelu *et al.* [9] consider the Canetti-Krawczyk adversary model and proposes a new efficient provably secure authenticated key agreement scheme for smart grid. Saxena and Grijalva [10] proposed a scheme with dynamic key distribution and secret key updating, which can generate a series of dynamic secrets on the communication network to generating keys for data encryption. However, most of these schemes are based on computationally expensive public-key cryptography which is impractical for the resource constrained smart meters.

In addition, the above communication schemes use the classical encryption and authentication algorithm. However, with the development of quantum computing, quantum computer poses a huge threat to the security of classic cryptography which used in power system. Shor's quantum algorithm solves the factorization problem of large integers and discrete logarithms in polynomial time. Grover's search algorithm allows for secondary acceleration when calculating the inverse hash function. Due to the further development of quantum cryptography, quantum key distribution technology is increasingly mature, and has risen from theory to practical. Considering the demands of power system for communication security, more and more researches are devoted to the application of quantum cryptography in the communication of power data to cope with the threat posed by quantum computers[11]–[15]. Zhou *et al.* [12] combined the quantum key distribution (QKD) system with the power vertical encryption authentication system to ensure the security of the communication. Xin and Xi [14] unified plaintext, ciphertext and key into a standard E1 interface signal, make the QKD to meet requirements of ''one-time pad'' (OTP) [15]. The channel in power system is not always ideal, Sharma *et al.* [16] verified that in collective noises environment the entangled-state-based protocols (such as ping-pong protocol) perform better than the single-qubit-based protocols. Naser [17] proposed a quantum authentication scheme based on entanglement swapping, completing authentication and communication tasks. Zawadzki *et al.* [18] improved the security of ping-pong protocol by using mutually unbiased basis in control mode. Yuan *et al.* [19] proposed quantum identity authentication based on ping-pong technique without entanglement to verify the legitimate user's identity and update the initial authentication key. To solve the problem of security of key in OTP, a new branch of quantum cryptography had emerged: quantum random number generators (QRNGs) [20]–[22]. Nikša Tadiá *et al.* [22] introduced a laser diode current with time dependence in 0.35-μm BiCMOS technology and could be used in optical QRNGs which used as the key generator in OTP.

In conclusion, the communication schemes proposed above for protecting data transmission of a power system has an expensive cost. At the same time, in the face of quantum computers, the integrity and confidentiality of power data cannot be well protected. Considering these factors, we introduce quantum key distribution protocol to improve the security of smart grid and propose a lightweight quantum cryptography scheme for power system. The scheme adopts the OTP mechanism and uses quantum cryptography to repair the defects in key generation and distribution in the classic stream cipher and realizes the secure transmission of power data.

The main contributions of this paper are as follows: (1) The QRNG generated session key is applied to OTP, which enhances the confidentiality of the transmitted data. (2) We designed an authentication algorithm and introduced it into the key distribution protocol. (3) The security analysis and experiments prove that this encryption method is more suitable for power system.

The rest paper is organized as follows: In Section 2, the combination of quantum cryptography and ''vertical encryption authentication'' system in the smart grid is introduced. In Section 3, the proposed communication scheme is described detailed. In Section 4, a series of theoretical analysis and experiments are carried out. In Section 5, conclusions are given.

II. QUANTUM CRYPTOGRAPHY FOR SMART GRID

The power secondary system is a vital part in smart grid which can ensure the security of the closed-loop monitoring system and the dispatch network. In order to ensure the reliability of the secondary power system, it is divided into three layers: control management layer, network communication layer, and field device layer. The network communication layer usually uses classical symmetric key to authentication and secure power data. In this paper, we use the quantum key instead of classical key to realize data encryption and authentication, as shown in Fig.1. The red line is a classical channel, while the blue line is a quantum channel, CA is communication agent.

Due to the differences between quantum key distribution system and power communication network, the system needs to add QKD session management module to connect QKD terminal and specific power equipment, such as data collector, to achieve the purpose of key distribution, identity authentication and message exchange. The system uses optical fiber channel as quantum channel to transmit qubit and key generation control system to control the generation and distribution of quantum key.

III. DATA SECURITY TRANSMISSION BASED ON QUANTUM ENCRYPTION

A. SECURITY TRANSMISSION SCHEME FOR POWER DATA

In this section, we describe a communication scheme based on quantum encryption, which is used to secure the

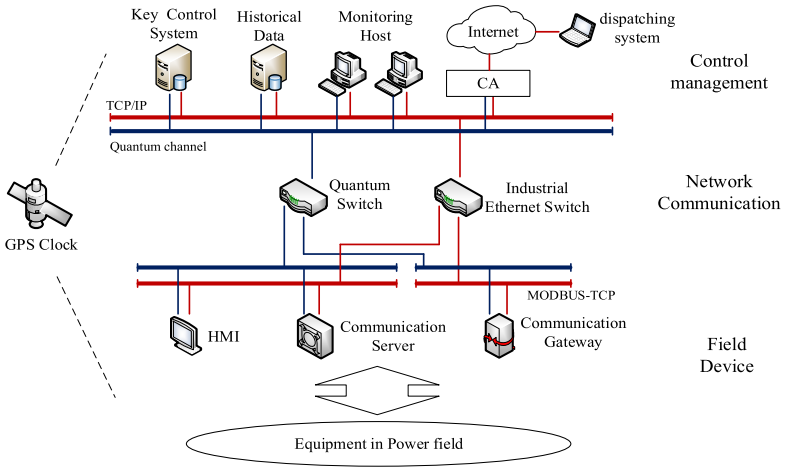

FIGURE 1. Power Communication network with QKD.

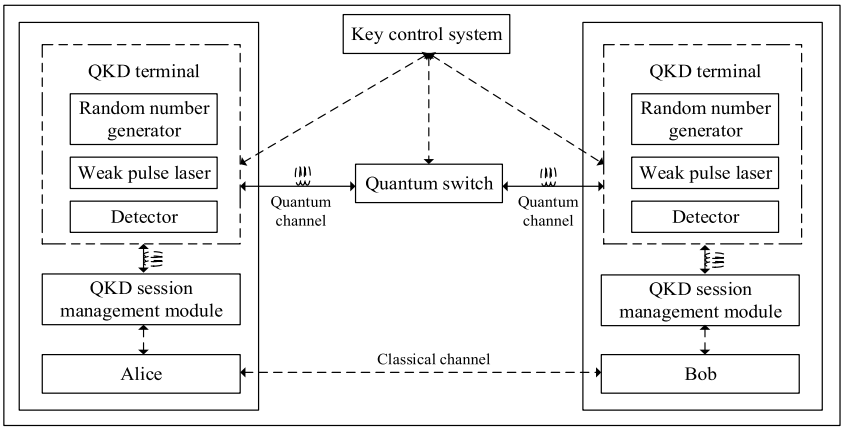

FIGURE 2. Lightweight quantum secure transmission scheme.

transmission of power data. In the scheme, we consider communication parties have a common secret S to each other which only known by both parties. S contains the identity information of both and is compiled into a binary. We combine OTP with quantum cryptography and use the QKD terminal to generate and distribute key. During the data transmission, the session key is generated by the QRNG in the QKD terminal and distributed by QKD protocol through the quantum channel, each key only is used once. And the identity authentication on both parties is based on S which is updated by session key. Assume that communication parties are Alice and Bob, the scheme is showed in Fig. 2.

The scheme consists of three processes: authentication, key distribution, data transmission. Since the quantum key distribution system is a transceiver split equipment, Alice and Bob each have their own a QKD terminal. The process is as follows:

1. As the communication requester, Bob sends a request to QKD_{Bob}.

2. After QKD_{Bob} accepts the request, it requests the secret S of Alice and Bob from key control system.

3. Key control system sends S to QKD_{Bob}. QKD_{Bob} generates the initial key and appends S, the ID of Bob to the end of it as the session key, then sends to Alice and Bob through quantum key distribution protocol.

4. QKD_{Alice} accepts the key and get the ID of Bob, then requests the secret S of Alice and Bob from key control system.

5. QKD_{Alice} accepts the S from control system, and compares the two S. If they are different, QKD_{Alice} rejects this communication. If same, then QKD_{Alice} sends session key to Alice

6. After Alice gets the session key, they can send messages to each other through the classical channel.

7. When communication over, use the session key to update S.

B. PREPARATION PHASE

In this section, we describe preparation phase of the proposed security transmission scheme, including key generation and distribution. Due to adopt the OTP mechanism, our scheme

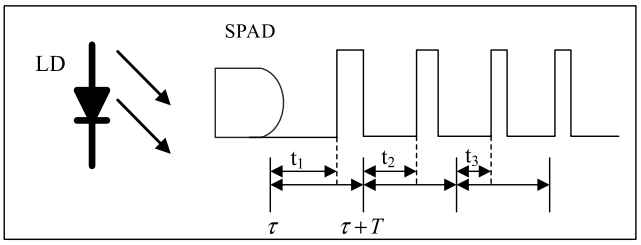

FIGURE 3. The QRNG which based on arrival time of photon.

uses the QRNG and QKD protocol to generate and distribute session key.

1) SESSION KEY GENERATION

In the OTP mechanism, the quality of the session key determines directly the security of the communication. The quality of the random number generated by the traditional random number generator depends on the seed, and it has the defect of long-period correlation and may not pass the local randomness test. Considering these factors, we use the QRNG based on the photon arrival time to generate random number, which is shown in Fig. 3.

The seed of the random number generator is the arrival time t_i of the photons which is related to T. It is known that the process of the generation of photons by a radiated semiconductor is Poisson process. We assume that the LD can generate a continuous and stable coherent light source, the probability that the number of photons falling in the time interval $(\tau, \tau + T)$ is k is given by:

$$P\left[N\left(\tau+T\right)-N\left(\tau\right)\right]=\frac{e^{-\lambda T}\left(\lambda T\right)^{k}}{k!} \tag{1}$$

where λ is the average number of the photon per unit time.

Due to the number of incident photons obeys Poisson distribution, and if there is only one arrival photon in the time interval $(\tau, \tau + T)$, the arrival time is evenly distributed. Therefore, we consider that only a single photon arrives in the fixed length of time interval T and calculate the photon arrival time t_i related to T. By the conditional probability, photon arrival time can be demonstrated to be uniform:

$$P\left(\tau\leq t\leq t_i|N(T)=1\right)=\frac{P\left(\tau\leq t\leq t_i, N\left(T\right)=1\right)}{P\left(N\left(T\right)=1\right)} \tag{2}$$

where N(T) represents the number of photons that occur in the time interval T, $P\left(\tau \leq t \leq t_i, N\left(T\right)=1\right)$ is joint probability that a photon arriving in the (τ, t_i) and none in the $(t_i, \tau + T)$.

After the photons are passed through the attenuator, they are detected by a silicon single-photon avalanche diode. Because of the attenuator, the $N\left(T\right) > 0$ measured by SPAD, instead of $N\left(T\right) = 1$. However, under the condition of the small values of λ, the possibility of more than one arrival photon negligible. By the time, the probability of photon arrival $P\left(\tau \leq t \leq t_i, N\left(T\right) > 0\right)$ approximates $P\left(\tau \leq t \leq t_i, N\left(T\right) = 1\right)$. The above conditional probability Eq. (2) is valid.

The original random data which quantized from the perturbation signal has a certain degree of bias. We use the Toeplitz matrix algorithm based on the Fast Fourier Transform to extract the randomness. The process is as follow:

$$D_f = T_{m\times n}\cdot D_r \tag{3}$$

where $D_f = \left(f_1, f_2, \cdots, f_m\right)^T$, $D_r = \left(r_1, r_2, \cdots, r_n\right)^T$, the complexity is $O\left(n^2\right)$.

2) QUANTUM KEY DISTRIBUTION PROTOCOL

As an important protocol in QKD, ping-pong protocol uses the Bell state $\left|\Phi^+\right\rangle$ as a carrier for transmitting information, which can be used for key distribution. According to the entanglement characteristics of quantum, both parties involved in communication can extract information from the entangled state only if they possess simultaneously all the entangled state particles.

Assuming the two communication parties are Alice and Bob, then the process is shown as follow. Bob prepares the maximum entangled photon pair according to the number, one of the pairs denotes as "home" photon which keeps the confidential and is stored in the local, while the other is "travel" photon which is send to Alice. Alice enters the message and control mode with a certain probability respectively. When entering the message mode, Alice receives the particles and selects randomly one unitary operation from I_A and σ_A to encode all the information in A, where I_A is the unit operator, without any operation, representing the classical bit 0, and σ_A is the phase flip, flip the phase of $|\rangle_A$, representing the classical bit 1. After encoding, Alice sends the particle sequence back to Bob. The ping-pong protocol is shown in Fig. 4.

The two communication parties can switch the two modes by the protocol. Control mode is used to detect the existence of eavesdroppers in the channel. According to Bell state, the results of the measure results of qubits by Bob and Alice are reversed under ideal channel condition. Any deviation from that correlation indicates the presence of Eve. However, it is known the security of ping-pong protocol depends that the travel qubit remains always in the maximally mixed state, has nothing to do with the encoding of Alice. When Eve eavesdrops, he prepares two probes x and y in the state $\left|2\right\rangle_x \left|0\right\rangle_y$, where $\left|2\right\rangle$ is the vacuum state. After Bob receives the encoding quantum sequence returned by Alice, Eve makes the probes interact before and after encoding and extract some information about the encoding. It is proved by theory that the mutual information between Eve and Alice is the same as that between Alice and Bob. Therefore, we introduce the identity authentication into the protocol to ensure that the both parties are legal communicators.

3) IDENTITY AUTHENTICATION

According to the above QKD process, there is no identity authentication performed during the communication. In order to remedy the defect, this work uses the secret S shared by the Alice and Bob for identity authentication. The S is used to

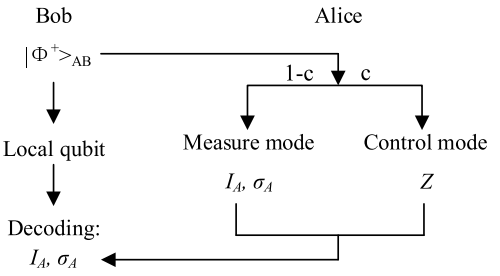

FIGURE 4. Ping-pong protocol.

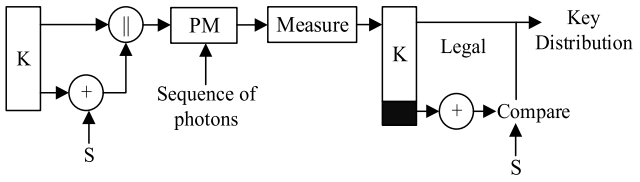

FIGURE 5. Authentication process between data collection terminal and center.

generate an authentication sequence and append at the end of the key. In addition, considering the noise and loss in quantum channel, we also append the check-code.

Suppose that the key generated by QRNG is $K = [k_1, k_2, \cdots, k_n]$, secret $S = [s_1, s_2, \cdots, s_n]$, then authentication sequence L which generate by the XOR of K and S is:

$$\begin{cases} L_1 = k_0 \oplus s_1 \oplus k_1 & if\ i = 1; \\ L_i = k_{i-1} \oplus s_i \oplus k_i & if\ i \geq 1; \end{cases} \tag{4}$$

where we stipulate that if $s_1 = 0$, then $k_0 = 1$, otherwise $k_0 = 0$.

Append L to the end of K and generate check code r_k and r_L of K and L respectively by the horizontal odd parity. Then append r_k and r_L to the end of it to get the sequence $K||L||r_K||r_L$. According to sequence, Bob sets the polarization direction of the photons and sends to Alice. Alice receives and chooses the measuring basis at random to measure the sequence and analyzes the results to judge whether the opponent is legal. If legal, communication is continuing, otherwise reject. The process is shown in Fig. 5.

Since only legitimate communicators know the secret S and measurement base, so it can verify the identity of both parties through the above process. In order to ensure the absolute security of identity authentication, after data communication is completed, the key generation control system uses the session key K to update S:

$$S = K \oplus S \tag{5}$$

Therefore, each S is used only once to resist the impersonation attack. At the same time, the introduction of the check code can reduce the rejection of communication caused by the channel noise to a certain extent. The measured sequence is decomposed into four parts: K, L, r_k, r_L. Use S to recover

Algorithm 1 Encryption

Initialization: $K = [k_1, k_2, \cdots, k_n]$, $S = [s_1, s_2, \cdots, s_n]$, M = m[p], j = 1, flag = 0;
  while (p-n) < 0 **do**
    for (i = 0; i < n; i++) **do**
      if (i+flag < p), **then** M_j [i] = m[i+flag ∗ n];
        else M_j [i] = 0;
      flag++; j++;
Construct permutation matrix s according to ascending order of S.
  if S[0] = 0, **then** $VIST = s$, $k_0 = 1$;
    else $VIST = s^{-1}$, $k_0 = 0$;
  for each $M_j = \{m_1, m_2, \cdots, m_i\}$ **do**
    replacement M_j according to $VIST$
    if j = 1, **then** $P_1 = k_0 \oplus m_1 \oplus k_1$
      else $P_i = P_{i-1} \oplus m_i \oplus k_i$
Replacement P according to $VIST$ to get C

K' from L:

$$\begin{cases} k_1 = L_1 \oplus k_0 \oplus s_1 & if\ i = 1; \\ k_i = L_i \oplus L_{i-1} \oplus s_i & if\ i \geq 1; \end{cases} \tag{6}$$

where we stipulate that if $s_1 = 0$, then $k_0 = 1$, otherwise $k_0 = 0$.

If there is a difference between K' and K, analysis the check code, and when there is only one error in the specified sequence, the communication is accepted. Therefore, communication is allowed when:

1. r_k matches with the key sequence, r_L doesn't and compared with K the K' has only two different bits, which is no error occurs in the key and one error in the L.

2. r_L matches with the key sequence, r_k doesn't and compared with K the K' has only one different bit, which is one error occurs in the key and no error in the L.

C. COMMUNICATION PHASE

1) LIGHTWAIGHT CRYPTOGRAPHIC ALGORITHM DESIGN

The OTP mechanism we used requires the length of the ciphertext, plaintext and key must be the same. Considering the performance of algorithm and the requirement of power system, our paper designs a stream cipher algorithm which is shown in Algorithm 1.

It is worth to certain that the length of the plaintext is variable. So it needs to be divided into sequences whose length is same as key's. According to the first bit of S, the permutation matrix and k_0 are generated. There are two permutations and a diffusion in our algorithm which can make the encryption results as complicated as possible.

2) PROCESS OF DATA ENCRYPTION AND DECRYPTION

According to the encryption algorithm described in the previous section the data encryption process is as follows:

1. QRNG generates the session key $K = [k_1, k_2, \cdots, k_n]$;

2. Plaintext M has p bit, and divides into n-bit data segment. If the length of last segment less than n, it would be filled with zero;

3. Construct the permutation matrix **s** according to the ascending order of S. If the first bit in S is zero, the final permutation matrix *VIST* is **s** and the value of k_0 is one, otherwise matrix *VIST* is the $\mathbf{s}^{-1}$ and k_0 is zero;

4. Permute M according to *VIST* to get m;

5. Encryption: if i = 1, then $P_1 = k_0 \otimes m_1 \otimes k_1$. If i > 1, then $P_i = P_i \otimes m_i \otimes k_i$;

[6. Permutation: permute P according to *VIST* to get C.

The process of decryption is:

1. Permutation: reverse permute C according to *VIST* to get P.

2. Decryption: if i = 1, then $m_1 = P_1 \otimes k_0 \otimes k_1$. If i > 1, then $m_i = P_{i-1} \otimes P_i \otimes k_i$;

3. Permutation: reverse permute m according to *VIST* to get M;

4. Remove the extra 0 in M to get the final plaintext;

IV. PERFORMANCE ANALYSIS AND COMPARISONS

A. RONDOMNESS ANALYSIS OF KEY

Considering that in actual use, the detection efficiency of silicon single-photon avalanche diode (Si-SPAD) is not ideal, and it is affected by the dead time, jitter, dark counts and the light during avalanche after the light pulse. The above factors will affect our Poisson statistics on photons and will ultimately affect the quality of the random numbers.

Autocorrelation analysis of the detector Si-SPAD gives the signal distribution after the light pulse and the dead time of the diode. The autocorrelation coefficient is calculated as:

$$R(i) = \frac{\langle X_i, X_T \rangle - \langle X_i \rangle \langle X_T \rangle}{\sqrt{\left(\langle X_i^2 \rangle - \langle X_i \rangle^2\right)\left(\langle X_T^2 \rangle - \langle X_T \rangle^2\right)}} \tag{7}$$

where X_i, X_T represent the detection signal of two moments when $t = t_i$ and $t = \tau + T$.

From (7) shows that the autocorrelation can't be ignored, that detection efficiency $\eta < 1$. Otherwise the detector has a count rate of 13.9Mcps, dead time of 45ns and dark counts occur at 100 to 500 times per second, which is about 15cps. Therefore, compared with the detection of photon flux, it is almost impossible for the dark counts, and the noise impact caused by the dark counts is negligible. Photon detection still follows the Poisson distribution. According to the analysis, (1) is revised as:

$$P[N(\tau + T) - N(\tau) = k] = \frac{e^{-\lambda T\eta}(\lambda T\eta)^k}{k!} \tag{8}$$

At the same time, multiphoton events will occur because the detected light source is attenuated continuous light. It is assumed that K photons appear in the time interval (τ, τ +T), and when the detector detects the first photon, it is inactivated immediately, that is, the dead time. Therefore, photons arriving in dead time will be discarded. In order to ensure that the detection event in each cycle is not greater than 1, the external reference period T we chose should be less than the detector dead time ensuring the stability and quality of random numbers.

In addition, the randomness of the sequence is quantified by minimum entropy, it is defined as follows:

$$H_\infty = -\log(\max P_i) \tag{9}$$

According to the above analysis, only the first photon is detected in the k photons reached in the interval (τ, $\tau + T$), that is, the probability $P(n = 1|k)$ is the largest. The value of P_1 is:

$$\begin{aligned} P_1 &= \sum_{i=0}^{k} p(n = 1|k)\, p(k) \\ &= \sum_{i=0}^{k} \frac{e^{-\lambda T\eta}(\lambda T\eta)^k}{k!}\left[1 - \left(1 - \frac{1}{T}\right)^k\right] \end{aligned} \tag{10}$$

So the minimum entropy is:

$$\begin{aligned} H_\infty &= -\log(\max P_i) \\ &= -\log(P_1) \geq \log(T) + \log(1 - e^{-\lambda T\eta}) - \log(\lambda T\eta) \end{aligned} \tag{11}$$

As can be seen from (10) and (11), the value of minimum entropy H_∞ depends on average photon number λ, external reference period T and Si-SPAD detection efficiency η. The above three parameters are related to the detector count rate C and dead time t_d:

$$C = \eta\lambda(1 - C \times t_d) \tag{12}$$

Therefore, the minimum entropy H_∞ is in the range of:

$$\begin{aligned} \log(T) + \log\left(1 - e^{-\frac{C}{1-C\times t_d}T}\right) - \log\left(\frac{C}{1 - C \times t_d}T\right) \\ \leq H_\infty \leq \frac{C/1 - C \times t_d}{1 - e^{-\frac{C}{1-C\times t_d}T}} \end{aligned} \tag{13}$$

According to (13), we can figure out that H_∞ is determined by the count rate of the single photon detector. From the perspective of autocorrelation and minimum entropy, we analyze the randomness of the sequences generated by QRNG. The analysis results show that each bit of the random sequence contains enough information and has good randomness, both have passed the dieharder test and the NIST test procedure.

B. SECURITY ANALYSIS OF PROTOCOL

According to the proposed scheme, the data collector performs the operation of the secret S and session key to generate the authentication sequence L, the sends the L and session key to the data service center. After receiving the message, the data service center parses out S' and compares it with the stored S to determine whether the source of the information is credible.

In the preparation phase, the data collection terminal C1 initiates a communication request, and its QKD terminal requests the key service center to send the secret S shared between C1 and the data service center. Key service center

sends the S to C1 and data service center. C1 and data service center transform S into the measurement bases sequence $M_L = \left\{M_{L_1}^1, M_{L_2}^2, \cdots, M_{L_n}^n\right\}$, for example, classic bit 0 corresponds to σ_z base and 1 corresponds to σ_x base. In addition, the measurement base used to obtain the session key is M which adopted in the EPR protocol. In scheme, C1 prepares entangled particle pairs according to the authentication sequence L:

$$\left|\varphi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} + |10\rangle_{AB}\right) \tag{14}$$

and sends the B particle to the data service center. According to protocol, C1 randomly selects the M to measure the A particle, data service center randomly selects M or M_L to measure B particle and send part of the results from the measurement basis M_L to C1. C1 uses Bell theory to detect whether there is an eavesdropper.

Data service center transforms the measurement result $|\Phi\rangle = M_L\,|\Psi\rangle = \{|\phi_1\rangle, |\phi_2\rangle, \cdots, |\phi_m\rangle\}\,(m \leq n)$ of the M_L into a classical quantum bit sequence L' and calculates L according to the algorithm, the compares them to determine whether C1 is a legitimate communicator or not. If it is legal, data service center uses session K encrypt L' and the corresponding sequence numbers N_i to get $C = E_k\left(L', N_i\right)$, send C to C1 via the classical channel. C1 decrypt C to get L' and N_i, then compares with its own measurement results to determine if the data service center is legal. Due to the two authentications, the attacker must know the shared secret S and the measurement results of the data center at the same time. However, this is very difficult. Therefore, the proposed scheme can effectively resist man-in-the-middle attacks.

C. PEFORMANCE COMPARSION OF SCHEME

In this section, we compare the proposed scheme with related smart grid communication schemes. The comparison includes security attributes and encryption algorithm performance.

The comparison of security attributes is shown in TABLE 1. It can be seen from the table that most communication schemes perform poorly in ensuring the security of session key and physical security of the data collectors and cannot resist the attack of the quantum computer. The security of session key determines the reliability of the power data. If the physical security of the data collector cannot be guaranteed, it may lead to the internal attacks on the collector. For quantum computer attacks, classical encryption algorithms, such as ECC-based and symmetric cryptographic algorithms, cannot resist. The proposed scheme uses quantum cryptography and the security of the session key does not depend on the computational complexity, it could resist the attack of quantum computers. And the OTP mechanism guarantees that each key is used only once, and the quantum key distribution protocol secure the distribution of the session key, so the replay and eavesdropping attacks invalid. Meanwhile, the authentication based on the S is bidirectional and S is updated after each communication, so it is difficult for the man-in-the-middle attack. Therefore, the proposed scheme can secure the transmission of power data.

TABLE 1. The security attributes comparison of different scheme.

Scheme	Proposed	EDAS [28]	P. Gope et al. [27]	Tsai et al. [8]	V. Odelu et al. [9]
S1	Yes	No	No	No	No
S2	Yes	Yes	Yes	Yes	Yes
S3	Yes	No	Yes	Yes	Yes
S4	Yes	Yes	Yes	Yes	Yes
S5	Yes	No	Yes	No	Yes
S6	No	No	Yes	No	No

S1: Protection against quantum attack; S2: Privacy against eavesdropper; S3: Protection against man-in-the-middle attacks; S4: Forward secrecy; S5: Session key security; S6: Physical security of the data collector

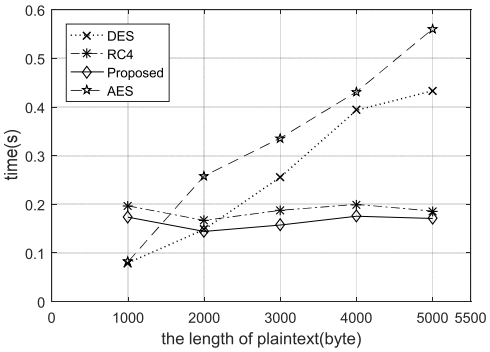

FIGURE 6. Time cost of the proposed algorithm.

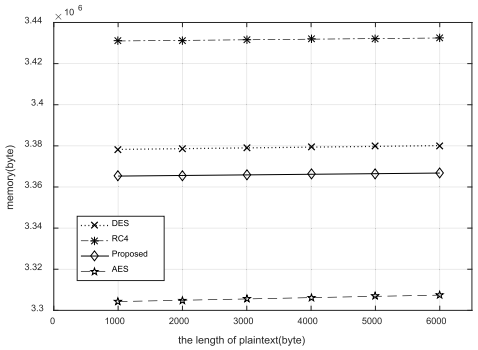

FIGURE 7. Memory cost of the proposed algorithm.

It can be seen from the above analysis that the identity authentication scheme can resist the man-in-the-middle attack and ensure the security and traceability of key distribution. For the encryption algorithm, the security of the key determines the security of the proposed encryption algorithm. Therefore, this part compares the performance of Algorithm 1 with the other three classic encryption algorithms.

We analyze four encryption algorithms on a 64-bit PC with win10 and Inter7 Core processor i7-3612QM. We select five different sets of keys and plaintexts during the experiment, and the experimental result is the average value. The key length of the DES is 64 bits (including the 8-bit check digit),

the key length of the AES is 256 bits, and the key length of RC4 and the encryption algorithm proposed in this paper is 256 bits. The keys and plaintexts are generated by the random function to avoid the contingency from artificially generated data.

Count the running time of the four algorithms to obtain the time taken for the whole cycle from the calling to the running, as shown in Figure 6. As can be seen from the figure, the classical symmetric encryption algorithms DES and AES grow linearly with the increase of the plaintext length, and the time of AES is shorter than DES. And the time of the stream cipher algorithm under different plaintext lengths is generally stable between 0.15 and 0.2. In summary, compared with the classic encryption algorithm, the stream encryption algorithm proposed has lowest cost of time.

Statistics four algorithms occupied memory during the lifetime, including the temporary memory, as shown in Figure 7. It can be seen from the figure that the occupied memory of the four algorithms shows a linear growth. Among them, the memory required for the RC4 algorithm is the largest, followed by the DES algorithm and the smallest AES algorithm, and the algorithm we propose is between the DES and the AES.

According to the relationship between the time cost and the space cost of the algorithm, if you reduce the time complexity, you must pay for the space, and vice versa. For an algorithm, you cannot have both. As shown in the experimental results, the cost of AES algorithm is the least, but the time cost is the hugest. The RC4 algorithm has the hugest space cost, the lower time cost, and the DES is between AES and RC4. The algorithm proposed in this paper has the lowest time cost and intermediate-level space cost. Compared with the above three encryption algorithms, our algorithm has achieved the best comprehensive time performance and spatial performance.

V. CONCLUSION

This paper presents a scheme of secure transmission of power big data based on lightweight quantum cryptography, which realizes the application of quantum cryptography in power environment. The quantum key generator and key distribution protocol are used to improve the communication mode of traditional power system and the key space in big data environment. This scheme is also applicable to other scenarios where it is necessary to protect the transmitted data. However, our proposed scheme can guarantee the security of key distribution, but the process is complicated. At present, there are still many problems to be solved in the practical application of quantum cryptography. In the future, we will simplify the process of key distribution and further improve real-time performance on the premise of ensuring the security of keys.

REFERENCES

[1] J. Hu, H. R. Pota, and S. Guo, "Taxonomy of attacks for agent-based smart grids," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1886–1895, Jul. 2014.
[2] N. Bui, A. P. Castellani, P. Casari, and M. Zorzi, "The Internet of energy: A Web-enabled smart grid system," *IEEE Netw.*, vol. 26, no. 4, pp. 39–45, Jul. 2012.
[3] C. Tu, X. He, Z. Shuai, and F. Jiang, "Big data issues in smart grid—A review," *Renew. Sustain. Energy Rev.*, vol. 79, pp. 1099–1107, Nov. 2017.
[4] S. Fries, H. J. Hof, T. Dufaure, and M. G. Seewald, "Security for the smart grid–enhancing IEC 62351 to improve security in energy automation control," *Int. J. Adv. Secur.*, vol. 3, pp. 169–183, Jan. 2011.
[5] V. C. Gungor *et al.*, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.
[6] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC-based self-certified key distribution scheme for the smart grid," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 7996–8004, Oct. 2018.
[7] A. P. Premnath, J.-Y. Jo, and Y. Kim, "Application of NTRU cryptographic algorithm for SCADA security," presented at the 11th Int. Conf. Inf. Technol., New Gener., Las Vegas, NV, USA, Apr. 2014, pp. 341–346.
[8] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, Mar. 2016.
[9] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2018.
[10] N. Saxena and S. Grijalva, "Dynamic secrets and secret keys based scheme for securing last mile smart grid wireless communication," *IEEE Trans. Ind. Informat.*, vol. 13, no. 3, pp. 1482–1491, Jun. 2017.
[11] B. Zhao *et al.*, "A novel NTT-based authentication scheme for 10-ghz quantum key distribution systems," *IEEE Trans. Ind. Electron.*, vol. 63, no. 8, pp. 5101–5108, Aug. 2016.
[12] J. Zhou, L. Lu, Y. Lei, and X. Chen, "Research on improving security of protection for power system secondary system by quantum key technology," *Power Syst. Technol.*, vol. 38, no. 6, pp. 1518–1522, 2014.
[13] Y. Ma, X. Wang, and D. Cui, "Secure communication mechanism for smart distribution network integrated with subcarrier multiplexed quantum key distribution," *Power Syst. Technol.*, vol. 11, p. 036, Nov. 2013.
[14] M. Xin and C. Xi, "Quantum logic circuit of quantum bit error correction coding and decoding for quantum communication in smart grid substation," *Zhongguo Dianji Gongcheng Xuebao/Proc. Chin. Soc. Electr. Eng.*, vol. 34, no. 25, pp. 4359–4363, 2014.
[15] M. Xin, Z. Liang, P. Ma, N. Jin, and M. Zhu, "Optical fiber transmission solution of measurement and control signal between substations based on quantum key distribution and one-time pad," *Autom. Electr. Power Syst.*, vol. 41, no. 12, pp. 212–230, 2017.
[16] V. Sharma, K. Thapliyal, A. Pathak, and S. Banerjee, "A comparative study of protocols for secure quantum communication under noisy environment: Single-qubit-based protocols versus entangled-state-based protocols," *Quantum Inf. Process.*, vol. 15, no. 11, pp. 4681–4710, 2016.
[17] M. Naseri, "Revisiting quantum authentication scheme based on entanglement swapping," *Int. J. Theor. Phys.*, vol. 55, no. 5, pp. 2428–2435, 2016.
[18] P. Zawadzki, Z. Puchała, and J. A. Miszczak, "Increasing the security of the ping–pong protocol by using many mutually unbiased bases," *Quantum Inf. Process.*, vol. 12, no. 1, pp. 569–576, 2013.
[19] H. Yuan, Y.-M. Liu, G.-Z. Pan, G. Zhang, J. Zhou, and Z.-J. Zhang, "Quantum identity authentication based on ping-pong technique without entanglements," *Quantum Inf. Process.*, vol. 13, no. 11, pp. 2535–2549, 2014.
[20] A. Martin, B. Sanguinetti, C. C. W. Lim, R. Houlmann, and H. Zbinden, "Quantum random number generation for 1.25-GHz quantum key distribution systems," *J. Lightw. Technol.*, vol. 33, no. 13, pp. 2855–2859, Jul. 1, 2015.
[21] M. Nakazawa *et al.*, "QAM quantum noise stream cipher transmission over 100 km with continuous variable quantum key distribution," *IEEE J. Quantum Electron.*, vol. 53, no. 4, Aug. 2017, Art. no. 8000316.
[22] N. Tadić, B. Goll, and H. Zimmermann, "Laser diode current driver with $(1 - t/T)^{-1}$ time dependence in 0.35-μm BiCMOS technology for quantum random number generators," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 64, no. 5, pp. 510–514, May 2017.
[23] P. Zawadzki, *Improving Security of the Ping-Pong Protocol*. Norwell, MA, USA: Kluwer, 2013.
[24] K. Thapliyal, A. Pathak, and S. Banerjee "Quantum cryptography over non-Markovian channels," *Quantum Inf. Process.*, vol. 16, no. 5, p. 115, 2017.
[25] P. Zawadzki, "Security of ping-pong protocol based on pairs of completely entangled qudits," *Quantum Inf. Process.*, vol. 11, no. 6, pp. 1419–1430, 2012.

[26] V. Sharma, U. Shrikant, R. Srikanth, and S. Banerjee, "Decoherence can help quantum cryptographic security," *Quantum Inf. Process.*, vol. 17, p. 207, Aug. 2018.
[27] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Trans. Smart Grid*, to be published.
[28] P. Gope and B. Sikdar, "An efficient data aggregation scheme for privacy-friendly dynamic pricing-based billing and demand-response management in smart grids," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3126–3135, Aug. 2018.

YUANCHENG LI received the Ph.D. degree from the University of Science and Technology of China, Hefei, China, in 2003. From 2004 to 2005, he was a Postdoctoral Research Fellow with the Digital Media Lab, Beihang University, Beijing, China. From 2009 to 2010, he was a Postdoctoral Research Fellow with the Cyber Security Lab, College of Information Science and Technology, Pennsylvania State University, PA, USA. Since 2005, he has been with North China Electric Power University, where he is currently a Professor and the Dean of the Institute of Smart Grid and Information Security.

PAN ZHANG was born in Baoding, Hebei, China, in 1989. He received the B.S. and M.S. degrees in computer science and technology from North China Electric Power University, Beijing, in 2014.

He is currently pursuing the Ph.D. degree in information security with North China Electric Power University. He is currently with the State Grid Information and Telecommunication Branch. He has authored more than five articles and more than four inventions. His research interests include information security, big data analysis, machine learning, and artificial intelligence.

RONG HUANG was born in Guizhou, China, in 1995. She received the B.S. degree in information security from North China Electric Power University, Beijing, in 2017.

She is currently pursuing the M.S. degree in information security with North China Electric Power University. Her research interests include machine learning and artificial intelligence, big data analysis, and quantum cryptography in smart grid.