基于嵌入式的分布式光伏系统数据加密研究

周玮[1]，纪元[1]，贾婷[1]，顾锡华[1]，秦奕[1]，毕思博[2]
（1.国网江苏省电力有限公司无锡供电分公司，江苏 无锡 214061；
2.江苏省电力有限公司信息通信分公司，江苏 南京 210024）

摘要：为保证基于嵌入式的分布式光伏系统数据的安全，针对嵌入式计算资源有限的问题，在128位AES加密算法的基础上，提出了一种轻量化加密算法。首先，针对AES轮函数进行优化，减少包含列混合的轮数；其次，通过轻量化优化列混合、密钥扩展2个步骤，设计轻量化AES加密算法；最后，搭建AES实验仿真平台，对轻量化AES加密算法进行实验分析，验证改进后加密算法的效率和安全性。实验表明，轻量化AES加密算法与AES加密算法相比较，在保证信息传输安全的同时，加密、解密速度可提升19.50%。

关键词：AES加密算法；轻量化；分布式光伏；嵌入式
中图分类号：TM28 **文献标识码**：A **DOI**：10.19457/j.1001-2095.dqcd25978

Embedded-based Data Encryption Research for Distributed Photovoltaic System

ZHOU Wei[1]，JI Yuan[1]，JIA Ting[1]，GU Xihua[1]，QIN Yi[1]，BI Sibo[2]
（1.*State Grid Jiangsu Electric Power Co.，Ltd. Wuxi Power Supply Branch*，*Wuxi* 214061，*Jiangsu*，*China*；2.*State Grid Jiangsu Electric Power Co.，Ltd. Information and Communication Branch*，*Nanjing* 210024，*Jiangsu*，*China*）

Abstract：In order to ensure the security of embedded-based distributed photovoltaic system data，a lightweight encryption algorithm was proposed on the basis of 128-bit advanced encryption standard（AES）for the problem of limited embedded computing resources. Firstly，the AES round function was optimized to reduce the number of rounds containing column mixing；secondly，the lightweight AES was designed through two steps：lightweight optimization of column mixing and key expansion；finally，the AES experimental simulation platform was set up to experiment and analyze the lightweight AES，and to validate the efficiency and security of the improved encryption algorithm. The experiments show that the lightweight AES，compared with the AES encryption algorithm，can improve the encryption and decryption speed by 19.50% while ensuring the security of information transmission.

Key words：advanced encryption standard（AES）encryption algorithm；lightweight；distributed photovoltaic；embedded-based

近年来，为解决能源短缺与环境污染的问题，新能源产业快速发展，分布式光伏设备得到了广泛的应用[1]。随着大量分布式光伏设备的投入，分布式光伏信息传输安全需要得到保证，若其敏感的数据信息泄露将会留下严重的安全隐患[2]。尽管计算机系统安全水平得到了明显提升，不过电力系统中的计算机系统网络安全水平与业界的要求尚有一定差距，随着大量的分布式资源接入配电台区，配电通信网络存在诸多安全隐患[3]。由于大多分布式光伏设备的处理器采用嵌入式系统，存在设备计算能力较弱、效率低的问题[4]。因此，需要一种速度快、效率高的轻量化信息加密算法，并保证加密的安全性[5]。

AES（advanced encryption standard）是一种对称加密算法，在1998年由J Daemen等提出，于2001年由美国国家标准和技术研究所（NIST）颁布[6]。文献[7]针对嵌入式系统，设计出基于软件的轻量化AES加密方案，将AES操作转成查表操

基金项目：国网江苏省电力有限公司科技项目（J2023111）
作者简介：周玮（1987—），男，硕士，高级工程师，主要研究方向为电力通信，Email：lyricse@126.com
通讯作者：纪元（1977—），男，硕士，高级工程师，主要研究方向为电力通信，Email：yuan_ji_1977@126.com

作，并优化内存访问机制，实现了嵌入式设备的加密通信系统，所提方案在不影响系统安全的同时，加解密效率可提升15.02%。文献[8]针对物联网产品缺乏安全机制的问题，对AES进行数据路径和密钥扩展优化，实现低功耗低能耗高安全的物联网应用。文献[9]针对浮空器平台在数据传输中受到自身处理器限制的问题，设计以七次轮函数为核心的轻量化AES加密算法的数据加密方案，在保证数据安全的同时提高算法的运行效率。文献[10]通过对数据进行预处理，简化字节代换，减少加密轮数，实现轻量化AES加密算法，加密效率提高了10%，解密效率提高了9.3%。文献[11]中的轻量化AES在有限域GF(2^4)上进行计算，减少了S-box和相应的Inv S-box，使得算法具有更快的计算速度。文献[12]提出了一种用于智能电网的轻量级匿名身份验证和密钥协商方案，该方案先使得智能电表和服务提供商进行相互身份验证然后建立共享会话密钥。文献[13]提出了一个轻量级基于密码认证密钥交换协议方案，该方案使用一种基于对称同态密码体制的新聚合方法，来保证用户用电量数据的机密性和完整性以及用户身份的隐私。

基于嵌入式的分布式光伏系统存在计算资源有限的问题，传统加密算法不能满足需求，因此需要一种轻量化加密算法适用于分布式光伏系统。本文基于128位AES加密算法，通过轮函数、列混合、密钥扩展的优化，减少计算量、降低资源消耗，实现算法的高效性和轻量化，适用于基于嵌入式的分布式光伏系统。

1　分布式光伏系统

1.1　分布式光伏网络拓扑结构

分布式光伏系统包括融合终端、分布式光伏设备和信息安全接入装置，如图1所示。分布式光伏设备所产生的电能接入到台区，与10 kV电网一起为台区用户提供能源，组成了一个完整的新能源供电系统。融合终端基于HPLC和LORA通信技术，通过信息安全接入装置，实现与分布式光伏设备的远距离安全信息交互。

目前由于台区端设备的不断接入，由不同厂家生产的设备所使用的协议不同以及属性数据表达不同，导致台区采集的数据表达无法统一[14]。基于此，提出分布式光伏接入技术方案，如图2所示，达到高效的应用集成和数据共享的目的。结

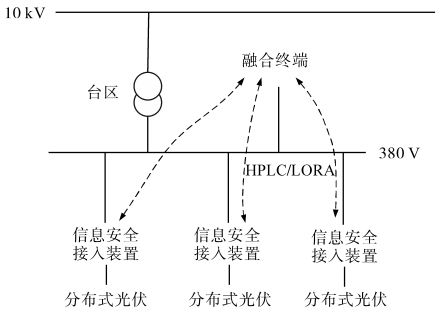


图1　分布式光伏系统结构

Fig.1　Distributed PV system structure

合分布式光伏设备的特点，建立分布式光伏信息模型，从分布式光伏的静态属性、动态属性、消息以及服务等主题进行设计规范，从命名、描述、访问模式、数据类型、调用方式等方面进行约束，搭建信息模型的整体架构；其次，采取Json文件格式对信息模型进行统一描述，构建分布式光伏终端设备的信息模型；最后，以MODBUS通信协议为基础，基于自注册信息交互机制，制定信息模型到标准通信协议的映射机制，实现分布式光伏与配电网的信息交互与指令下达。

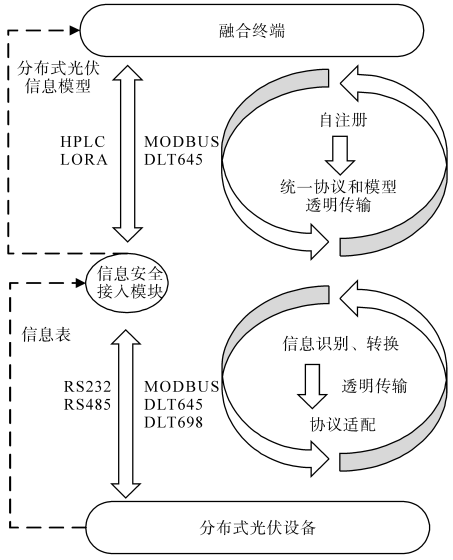


图2　分布式光伏接入技术方案

Fig.2　Distributed PV access technology program

1.2　分布式光伏加密系统

针对分布式光伏系统信息存在的潜在数据泄露风险，以及光伏通信设备计算能力与存储空间存在客观限制的现状，根据现有对称及非对称加密算法在较低计算能力的物联网设备上的研究现状，根据加密算法软件和硬件实现方式，从处理器占用率、算法运算时间、存储空间使用量、算法安全强度等多个维度选择对称加密(AES128)和非对称加密(RSA)混合使用的加密

方式[15]。如图3所示，分布式光伏设备通过AES和RSA实现在融合终端的注册，最终通过AES加密算法实现两者间的信息交互。

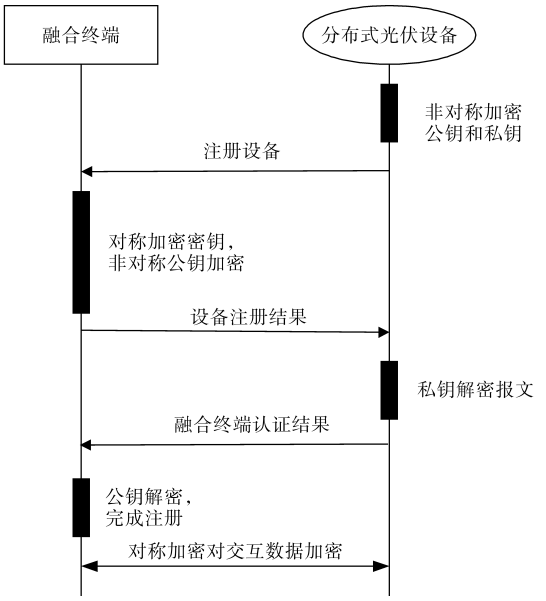


图3　分布式光伏网络拓扑结构

Fig.3　Distributed PV network topology

本文加密对象是分布式光伏设备在融合终端完成注册后的交互信息，信息交互主要基于DL/T 645通信协议。DL/T 645协议支持设备的数据读取、控制和管理等功能，基于此通信协议的加密数据主要包括分布式设备状态信息（电量、功率、电压、电流等）和操作命令（读取、控制和配置等），要求能够进行实时的加密信息传输，具有较强的实时性。因此在AES的基础上，对其进行轻量化研究，实现基于嵌入式的分布式光伏系统的高效率加密。

2　轻量化AES加密算法

2.1　AES加密算法原理

AES是目前应用最为广泛的一种对称加密算法，加密、解密使用相同的密钥。AES也是一种分组密码，将明文分组，每个分组的长度都是相同的，一次对一组数据集进行加密，直至整个文本被加密为止。在AES中，明文分组的长度仅为128位[16]。密钥的长度可以设置为128位、192位或256位，不同长度的密钥推荐的加密轮数有所不同，具体如表1所示。

AES的整体结构如4图所示，其中的$W[0,3]$是指$W[0]$，$W[1]$，$W[2]$和$W[3]$串联组成的128位密钥。在10轮操作之前，先将明文和原始密钥进行一次异或加密操作。加密的第1~9轮的加密轮函数一样，包括4个操作：字节代换、行位移、列混合和轮密钥加。在最后一轮的迭代中，不执行列混合。解密的第1轮到第9轮的轮函数也是一样，包含：逆字节代换、逆行位移、逆列混合和轮密钥加，最后一轮迭代不执行逆列混合。

表1　AES加密算法分类

Tab.1　Classification of AES

AES	密钥长度	分组长度	加密轮数
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

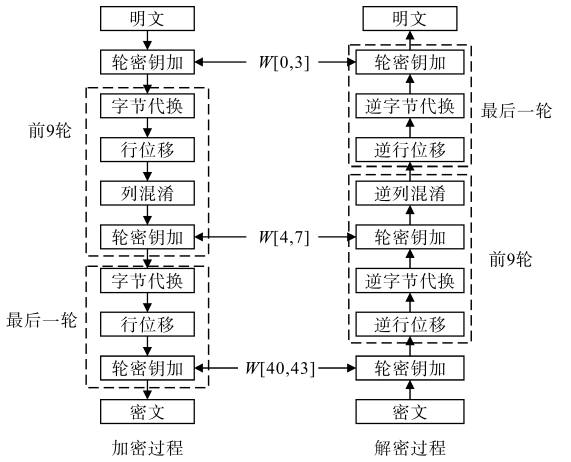


图4　AES加密算法流程

Fig.4　AES encryption algorithm process

2.2　轻量化AES

2.2.1　轻量化轮函数

AES-128中轮函数的轮数为10轮，算法前9轮的步骤一样，加密最后一轮不包含列混合，减少了AES加密算法的线性关系的同时，提高了AES的效率[17]。轻量化AES加密算法加密流程如图5所示。

列混合操作是AES算法中的一个重要步骤，

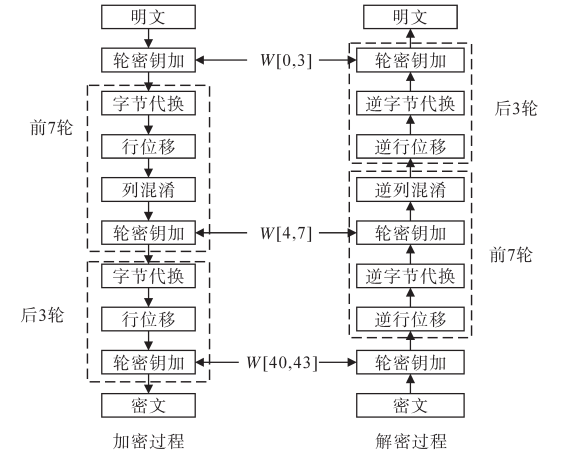


图5　轻量化AES加密算法流程图

Fig.5　Lightweight AES encryption algorithm process

它涉及矩阵运算和复杂的数据变换，需要消耗较多的计算资源。在轻量化AES加密算法中，省略最后3轮的列混合可以显著减少计算负担，从而提高加密和解密操作的效率。在资源受限的分布式光伏系统中，轻量化AES算法能够更好地适应这些环境，提供更快速、更流畅的加密服务。

2.2.2　轻量化行位移

AES算法中行移位是对状态矩阵的每一行进行向左的移位操作，当使用的密钥长度为128位时，行移位操作如图6所示。

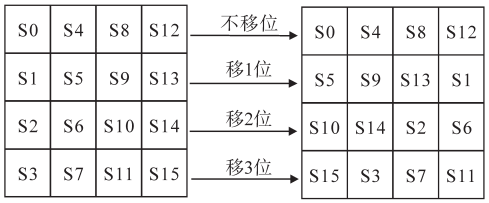


图6　AES加密算法行位移

Fig.6　Row shift of AES

轻量化AES加密算法中将行位移进行整列位移，每1列向右位移R字节，R为当前加密的轮数，不使用每行进行不同移位的方法，使得移位轻量化。如图7所示，当R=1时，状态矩阵每一列向右移动1位。整列位移减少了数据重新排列的需要，减少资源的消耗，从而提高了计算效率。

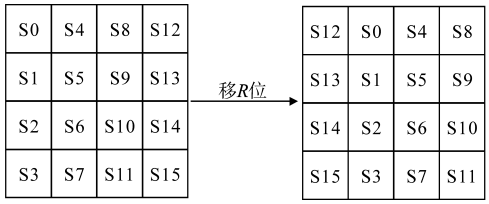


图7　轻量化AES加密算法列位移

Fig.7　Row shift of lightweight AES

2.2.3　轻量化密钥扩展

AES加密算法中需要进行11次轮密钥加操作，轮密钥加是将轮密钥与状态矩阵中的数据通过异或操作产生新的状态矩阵，是由$W[4i]$，$W[4i+1]$，$W[4i+2]$，$W[4i+3]$组成的44列数组，其中$W[0]$，$W[1]$，$W[2]$，$W[3]$是由密钥得出的初始数组，对其进行密钥扩展，得出完整密钥数组，扩展方式如下：

1）如果i不是4的倍数，那么密钥扩展公式如下：

$$W[i]=W[i-4]\oplus W[i-1] \tag{1}$$

2）如果i是4的倍数，那么密钥扩展公式如下：

$$W[i]=W[i-4]\oplus T(W[i-1]) \tag{2}$$

其中，函数T由3部分组成：字循环、字节代换和轮常量异或。

轻量化密钥扩展省去对i是否为4的倍数的特殊处理，可以简化密钥扩展的流程，减少算法中的分支和条件判断，使得算法结构更加清晰和统一，减少一些不必要的计算步骤和内存访问，从而提高密钥扩展的执行效率。扩展方式如下：

$$W[i]=W[i-4]\oplus W[i-1] \tag{3}$$

3　实验验证与分析

为了验证本文所设计的轻量化AES加密算法的性能，基于Matlab 2021b实现加密算法信息熵、雪崩效应和加密效率的仿真实验分析，基于以STM32F407为处理器的分布式光伏设备进行加密算法加密效率的进一步分析，验证本文所设计的轻量化AES加密算法的安全性和高效性。

3.1　信息熵分析

信息熵反映信息中的不确定性，是一种衡量数据随机性和不可预测性水平的指标。信息熵可以作为加密算法安全性分析的一个指标。如果加密算法在加密过程中能够有效地扩散和混淆明文的信息，使得密文的信息熵显著增加，那么算法的安全性通常也会更高。在加密算法中，信息熵是衡量数据在加密前后的信息量以及加密算法的强度的指标，信息的熵值越大就表明密文数据中所包括的有用内容也就越少，信息熵计算公式如下[18]：

$$H(m)=-\sum_{i=0}^{2^n-1}p(m_i)\log_2 p(m_i) \tag{4}$$

式中：n为随机变量m所有可能取值的个数；$p(m_i)$为随机变量m取第i个值的概率。

密文数据中，每个字节值的取值范围在[0，255]之间。对于AES加密算法，由于其设计原理，期望的密文是伪随机的，因此理论上每个字节的值都应该是均匀分布的，信息熵应该接近其最大值8。

利用实验平台，AES加密算法和轻量化AES加密算法使用相同的密钥加密相同的明文数据集，获取100~1 000条明文加密后的密文数据的平均信息熵，并比较他们的信息熵的差值，如表2所示。根据表2可以得知，经过AES和轻量化AES加密后的密文信息熵都接近理想数值8，并且信息熵差值小于0.01。因此，可以证明本文设计的轻量化AES加密算法在加密过程中能够有效地扩散和混淆明文的信息，可以保证轻量化AES加密算法的安全性，能够有效地防止信息的

泄露。

表2 密文信息熵

Tab.2 Ciphertext information entropy

明文数量	信息熵		
	标准AES	轻量化AES	熵差
100	7.935 8	7.933 6	0.002 2
200	7.940 4	7.938 4	0.002 0
400	7.940 3	7.932 8	0.007 5
600	7.937 5	7.936 3	0.001 2
800	7.938 0	7.937 4	0.000 6
1 000	7.939 0	7.938 0	0.001 0

3.2 雪崩效应分析

雪崩效应是在加密算法中的一种属性，具体指的是，当输入（无论是密钥还是明文）发生最细微的改变时，会导致输出的剧烈改变。这种特性对加密算法至关重要，因为它确保了加密过程的高度敏感性和随机性。雪崩效应计算方式如下：雪崩效应=密文反转字节数/密文字节总数。

标准AES和轻量化AES使用相同的128位密钥加密一组明文，改变密钥中的1位再次加密，对雪崩效应进行分析，如表3所示。

表3 雪崩效应分析

Tab.3 Avalanche effect analysis

算法	总字节数	反转字节数	雪崩效应
标准AES	128	63.7	0.498
轻量化AES	128	67.5	0.527

由表3可知，轻量化AES加密算法在雪崩效应上优于标准AES加密算法，因此可以确保轻量化AES加密过程的高度敏感性和随机性，保证算法的安全性。

3.3 效率分析

加密算法的效率是加密算法性能的重要参数，主要看加密和解密所需要的时间。本文的主要目标是设计一种适用于嵌入式系统的轻量化AES加密算法，相比于标准的AES加密算法，本文所提出的算法需要在效率方面有很大的提升。本文通过仿真实验和硬件实验验证所提出的轻量化AES加密算法的高效率性。

3.3.1 仿真实验

实验一，AES加密算法和轻量化AES加密算法使用相同的密钥加密相同的明文数据集，获取100~1 000条明文加密后的密文数据的加密和解密所消耗的时长。如图8所示，轻量化AES加密算法加密和解密所消耗的时间都小于AES加密算法加密和解密的时间，并随着加密明文数量的增加时间差也逐渐增大。

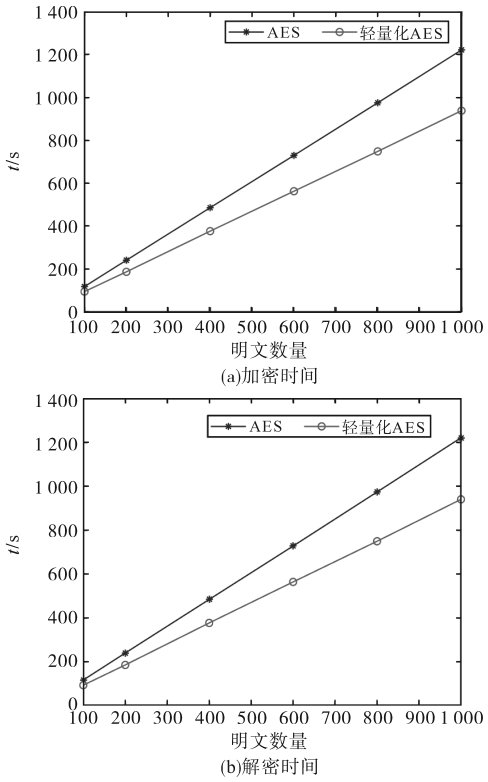


图8 仿真加密、解密时间

Fig.8 Simulation encryption and decryption time

实验二，AES加密算法和轻量化AES加密算法使用相同的密钥加密相同的明文，重复进行2 000次，获取加密和解密所消耗的平均时长，如图9所示。

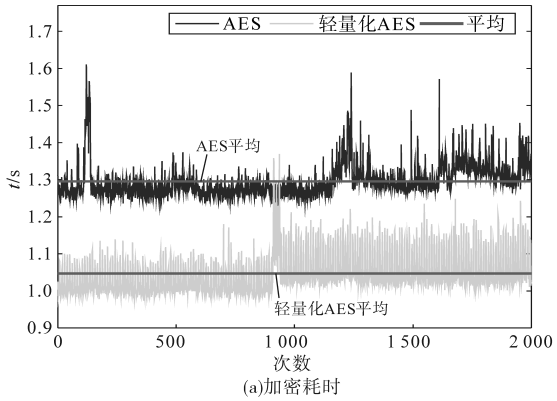
耗时比较结果如表4所示，AES加密算法轻量化前、后平均加密时间为1.298 6 s和1.046 9 s效率提升19.38%，轻量化前、后解密时间为1.289 6 s和1.046 6 s，效率提升18.84%。最终加密、解密合计效率提升19.11%，达到预期效果。

3.3.2 硬件实验

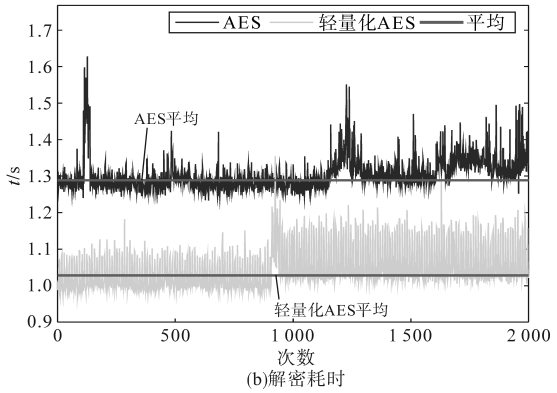
本文使用的分布式光伏设备的处理器采用Cortex M4内核的STM32F407，基于此进行加密算法效率实验，验证所提出的轻量化AES加密算法的高效率性。

AES加密算法和轻量化AES加密算法使用相同的密钥加密不同大小的明文数据源，获取加密、解密10~100 kB的明文数据源所消耗的时长。如图10所示，轻量化AES加密算法加密和解密所消耗的时间都小于AES加密算法加密和解密的时间，并随着加密明文数量的增加时间差也逐渐增大。

为了进一步分析加密算法在效率方面的提



(a)加密耗时



(b)解密耗时

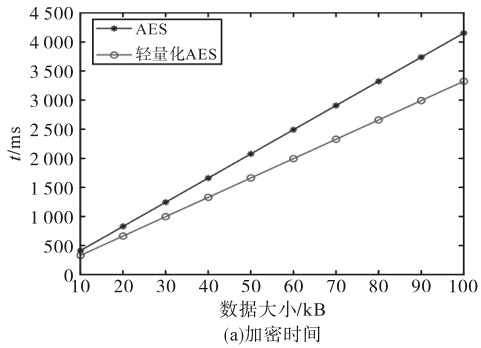
图9　轻量化AES与AES耗时对比

Fig.9　Comparison of time consuming lightweight AES with AES

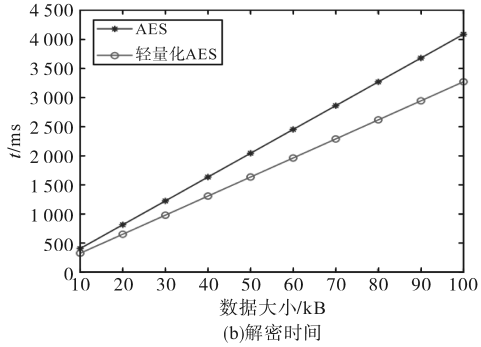
表4　轻量化AES与AES耗时比较

Tab.4　Time-consuming comparison of lightweight AES vs AES

加密方式	加密耗时/s	解密耗时/s	合计/s	优化
标准AES	1.298 6	1.289 6	2.588 2	19.11%
轻量化AES	1.046 9	1.046 6	2.093 5	



(a)加密时间



(b)解密时间

图10　硬件加密、解密时间

Fig.10　Hardware encryption and decryption time

升,表5为加密算法加密、解密10~100 kB明文数据源所消耗的具体时间,计算加密算法在不同大小数据效率的提升,取平均值。比较结果为:轻量化AES加密算法较标准AES加密算法加密效率提升19.947%,解密效率提升19.953%,综合提升19.50%。

表5　硬件中轻量化AES与AES耗时比较

Tab.5　Time-consuming comparison of lightweight AES vs AES in hardware

数据大小/kB	加密时间/ms			解密时间/ms		
	标准AES	轻量化AES	时间差	标准AES	轻量化AES	时间差
10	415	332	83	409	328	81
20	831	665	166	817	654	163
30	1 246	998	248	1 226	981	245
40	1 661	1 330	331	1 636	1 309	327
50	2 077	1 663	414	2 044	1 636	408
60	2 492	1 995	497	2 453	1 963	490
70	2 908	2 328	580	2 861	2 290	571
80	3323	2 660	663	3 270	2 618	652
90	3 738	2 993	745	3 679	2 944	735
100	4 154	3 325	829	4 087	3 270	817

3.4　运行内存分析

基于分布式光伏设备,使用轻量化AES加密算法和AES加密算法进行一轮加密和解密,统计运行内存占用情况,结果如表6所示。轻量化AES加密算法较标准AES加密算法运行内存少占用0.09 kB,性能提升1.5%。

表6　运行内存占用

Tab.6　Running memory consumption

加密方式	运行内存/kB	优化
标准AES	5.83	1.5%
轻量化AES	5.74	

4　结论

针对嵌入式分布式光伏系统数据安全中存在的问题,为了加密的高效性和安全性,提出轻量化AES加密算法,采用轻量化轮函数、轻量化行位移和轻量化密钥扩展的方案。一方面,通过AES加密算法和轻量化AES加密算法密文数据信息熵和雪崩效应的分析,验证了轻量化AES加密算法的安全性;另一方面,通过对比AES加密算法和轻量化AES加密算法的加密和解密所消耗的时间,可以体现轻量化AES加密算法的高效性。最终表明,相比于AES加密算法,轻量化AES加密算法在保证数据安全性的同时,加密效

率提高19.947%，解密效率提高19.953%，综合效率提高19.50%，有效地实现了分布式光伏系统信息加密的可靠性和高效性。

参考文献

[1] 曹炜，董浩洋，李芸，等. 分布式光伏高比例接入的国外经验及实践启示[J]. 电气传动，2022，52(4)：3-11.
CAO Wei，DONG Haoyang，LI Yun，et al. Foreign experience and practical enlightenment of the high proportion access of distributed photovoltaic high-proportion[J]. Electric Drive，2022，52(4)：3-11.

[2] 栗峰，丁杰，周才期，等. 新型电力系统下分布式光伏规模化并网运行关键技术探讨[J]. 电网技术，2024，48(1)：184-199.
LI Feng，DING Jie，ZHOU Caiqi，et al. Key technologies of large-scale grid-connected operation of distributed photovoltaic under new-type power system[J]. Power System Technology，2024，48(1)：184-199.

[3] 吴岩. 电力自动化通信技术中的信息安全分析[J]. 中国新技术新产品，2011(12)：25.
WU Yan. Analysis of information security in power automation communication technology[J]. New Technology & New Products of China，2011(12)：25.

[4] 曾小波，易志中，焦歆. 基于51核的AES算法高速硬件设计与实现[J]. 电子科技，2016，29(1)：36-39.
ZENG Xiaobo，YI Zhizhong，JIAO Xin. High-speed hardware design and implementation of AES algorithm based on 51 core [J]. Electronic Science and Technology，2016，29(1)：36-39.

[5] QASAIMEH M，Al-QASSAS S R，TEDMORI S. Software randomness analysis and evaluation of lightweight ciphers：the prospective for IoT security[J]. Multimedia Tools and Applications，2018，77(14)：18415-18449.

[6] BURR W E. Selecting the advanced encryption standard[J]. IEEE Security & Privacy，2003，1(2)：43-52.

[7] 刘政，代培培，邢建平，等. 面向嵌入式设备的轻量级AES加密通讯系统的设计与实现[J]. 电子器件，2023，46(1)：29-35.
LIU Zheng，DAI Peipei，XING Jianping，et al. Design and implementation of a lightweight AES encrypted communication system for embedded devices[J]. Chinese Journal of Electron Devices，2023，46(1)：29-35.

[8] BUI D H，PUSCHINI D，BACLES-MIN S，et al. AES datapath optimization strategies for low-power low-energy multisecurity-level internet-of-things applications[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems，2017，25(12)：3281-3290.

[9] 张馨方，周江华. 基于轻量型AES加密算法的浮空器平台数据传输方案[J]. 计算机测量与控制，2023，31(6)：183-190.
ZHANG Xinfang，ZHOU Jianghua. Data security transmission scheme of aerostat platform based on lightweight AES encryption algorithm[J]. Computer Measurement & Control，2023，31(6)：183-190.

[10] NICCOLÒ C，ANDREA T，CARLO D，et al. A secure real-time multimedia streaming through robust and lightweight AES encryption in UAV networks for operational scenarios in military domain[J]. Procedia Computer Science，2022，205：50-57.

[11] QASAIMEH M，AI-QASSAS R S，MOHAMMAD F，et al. A novel simplified AES algorithm for lightweight real-time applications：testing and discussion[J]. Recent Advances in Computer Science and Communications，2020，13(3)：435-445.

[12] ZHANG L，ZHAO L，YIN S，et al. A lightweight authentication scheme with privacy protection for smart grid communications [J]. Future Generation Computer Systems，2019，100：770-778.

[13] 关志涛，颜立，何杰涛，等. 面向智能电网的信息安全技术展望[J]. 智慧电力，2010，38(6)：5-8.
GUAN Zhitao，YAN Li，HE Jietao，et al. Prospect of smart grid-oriented information security technology[J]. Smart Power，2010，38(6)：5-8.

[14] 程凯，王鹏宇，包涛，等. 信息物理融合的电力系统日前-日内优化调度[J]. 电气传动，2023，53(10)：49-56.
CHENG Kai，WANG Pengyu，BAO Tao，et al. Day-ahead and intra-day optimal dispatching of cyber-physical integrated power system[J]. Electric Drive，2023，53(10)：49-56.

[15] 冷飞，徐进华，栾仕喜. RSA融合AES算法的网络信息安全方法[J]. 华侨大学学报(自然科学版)，2017，38(1)：117-120.
LENG Fei，XU Jinhua，LUAN Shixi. Research on network information security based on RSA fusion AES algorithm[J]. Journal of Huaqiao University (Natural Science)，2017，38(1)：117-120.

[16] 南亚会，刘继华，薛艳锋. 混沌参数调制下RSA数据加密算法研究[J]. 计算机测量与控制，2017，25(6)：203-206.
NAN Yahui，LIU Jihua，XUE Yanfeng. Under chaotic parameter modulation RSA data encryption algorithm research[J]. Computer Measurement & Control，2017，25(6)：203-206.

[17] 李升亮. 基于AES算法的光盘库数据加密技术研究与实现[D]. 武汉：华中科技大学，2015.
LI Shengliang. Research and implementation on data encryption for optical disc library based on AES[D]. Wuhan：Huazhong University of Science and Technology，2015.

[18] PREMKUMAR R，ANAND S. Secured and compound 3-D chaos image encryption using hybrid mutation and crossover operator[J]. Multimedia Tools and Applications，2019，78(8)：9577-9593.

收稿日期：2024-06-06
修改稿日期：2024-08-18