Low-Power AES Data Encryption Architecture for a LoRaWAN

KUN-LIN TSAI1, (Member, IEEE), FANG-YIE LEU2, (Member, IEEE), ILSUN YOU3, (Senior Member, IEEE), SHUO-WEN CHANG4, SHIUNG-JIE HU1, AND

1Department of Electrical Engineering, Tunghai University, Taichung 407, Taiwan
2Department of Computer Science, Tunghai University, Taichung 407, Taiwan
3Department of Information Security Engineering, Soochunhyang University, Asan 31538, South Korea

Corresponding author: Ilsun You (e-mail: ilsunu@gmail.com).
The work was supported by the Ministry of Science and Technology, Taiwan, R.O.C. under Grant no. MOST 107-2221-E-029-006 and by 'The Cross-Ministry Giga KOREA Project’ grant funded by the Korea government(MSIT) (No.GK19N0600, Development of 20Gbps P2MP wireless backhaul for 5G convergence service)

ABSTRACT In recent years, the Internet of Things (IoT) has significantly increased the number of Internet connections to a large number of objects in different domains, including industry, homes and transportation. The LoRaWAN developed by the LoRa Alliance is a long-range wide area network specification suitable for an IoT environment due to its low-power communication. It provides a star-of-stars topology, well-defined MAC layer protocol and three communication modes to further lower its power consumption and employs the Advanced Encryption Standard (AES) cryptography and several session keys to increase its network security. However, for battery powered IoT end nodes, the AES encryption process consumes some amounts of power owing to involving multiple cycles of repetition. To solve this problem, in this study, we propose a low power consumed AES encryption architecture, named Low-Power AES Data Encryption Architecture (LPADA), which reduces the power consumed by the AES for data encryption by using low power SBox, power gating technique and power management method. A key updating procedure is also proposed to increase the security of the session-key renewal. The system is simulated using the Synopsys library with five different supply voltages. The experimental results show that 62.0% of dynamic power reduction and 88.5% of leakage power lowering have been achieved compared to the power consumed by traditional AES data encryption. The security analysis also shows that the key updating procedure for the LPADA enables mutual authentication between end nodes and application servers, and resists replay attacks and eavesdropping attacks from hackers.

INDEX TERMS Low Power, AES, LoRaWAN, Power Gating, Power Management

I. INTRODUCTION
Recently, numerous Internet of things (IoT) based applications have been developed, including production logistics synchronization systems [1], smart factories [2], smart cities [3], healthcare [4] and smart grids [5]. Basically, IoT enables real world objects to collect data and to exchange data with each other. Using these data, system managers or servers can operate/control some specific devices to enhance our living environment. According to the Ericsson Mobility Report 2018 [6], more than 23.3 billion IoT-related devices will connect to the IoT network by 2023. Traditionally, a 4G network, Wi-Fi and Zigbee are used to connect IoT devices to their application platforms. However, some IoT applications, such as smart cities [7] and smart traffic [8], collect little data which are then transmitted to their application platforms over a long distance. So Low Power Wide Area Network (LPWAN) standards have been created to ensure reliable, secure, low-energy-consumption, and long distance IoT communication. NB-IoT (Narrow Band-IoT) [9], LoRaWAN [10], Sigfox [11], Weightless [12] and HaLow [13] are typical examples.
NB-IoT and LoRaWAN have been the subjects of many studies. The former standardized by 3GPP allows IoT devices to communicate with each other using licensed telecommunications bands. NB-IoT has many important features, such as long battery life for end nodes, massive connected IoT devices and low device cost. The latter developed by the LoRa Alliance uses unlicensed bands and the LoRa physical layer to define IoT communication protocols and network topology. The LoRaWAN also supports long range communication, ensures a long battery lifetime, secures data communication, and provides high network capacity. In general, a LoRaWAN architecture [10] consists of numerous end nodes, concentrators/gateways, network servers and application servers.

Although many security methods [14, 15] have been utilized to secure an IoT environment, the LoRaWAN uses Advanced Encryption Standard (AES) [16], a well-known encryption/decryption mechanism, to secure the payload of a message transmitted between an end node and its corresponding application server. The AES, which involves multiple cycles of repetition to perform one encryption consumes much energy for a battery-powered end node [17, 18]. Both McGrew [18] and Heer et al. [19] pointed out that complicated encryption algorithms should not be used in energy-constrained IoT devices. If IoT security is ensured, energy management may be often worse. Trappe et al. [20] showed that advanced cryptography algorithms are not suited to IoT devices with limited energy and memory space because these algorithms often require a large storage space and strong computing capability. To reduce the energy consumption of IoT devices, Tsai et al. [21] proposed a LADE method that provides a simple but secure data communication method. Although the LADE presented a simple process for end devices, the security level of the LADE needs to be verified. In other words, the energy-efficiency, performance and security in an IoT environment ought to be balanced.

Generally, the end nodes of an IoT system are usually resource-constrained, in that they have limited energy, processing capability and memory capacity. This study proposes a low-power security scheme, called Low-Power AES Data Encryption Architecture (LPADA), to reduce the power consumed by AES. The LPADA maintains the security of AES, but controls encryption/decryption power by using low-power SBox, power gating and power management techniques. A key updating procedure is also proposed in the LPADA to enable better key management.

Besides, a low-power hardware AES circuit is implemented. Generally, the hardware performs AES well and consumes less power [22]. But it requires extra manufacturing costs. Software that runs on a processor requires thousands of instructions to complete one AES encryption/decryption process and consumes much more power than hardware does. Since AES is a basic and regular operation in LoRaWAN’s end nodes, this study decreases power consumed by these end nodes by using our proposed method. Simulations are performed using the Synopsys 32nm cell library with 5 different supply voltages. The experimental results show there is 62.0% of reduction in the dynamic power and 88.5% of reduction in the leakage power over a traditional AES data encryption architecture. The security analysis also shows that the key updating procedure for the LPADA enables mutual authentication between end nodes and servers and resists replay attacks and eavesdropping attacks.

The contributions of this paper are as follows.
1. Three low power techniques are used to implement an AES encryption/decryption hardware so as to significantly reduce the power consumed by the LoRaWAN end nodes.
2. Instead of inflexible combinational circuitry, a content addressable memory based SBox is developed for the LPADA to support AES encryption/decryption-key update procedure.
3. A secure key updating procedure is proposed to increase the security of session-key renewal.
4. Multiple operating voltages are employed to estimate the power consumption of the proposed LPADA and to provide a design trade-off between power consumption and performance.

The remainder of the paper is organized as follows. Section II introduces preliminary knowledge and related studies of this paper. Section III details the proposed LPADA and Section IV describes the experimental results. The security analysis and a discussion are presented in Section V. Section VI concludes this study and details opportunities for future study.

II. PRELIMINARY
This section describes the security scheme for a LoRaWAN, the encryption process for AES and some studies related to this paper.

A. LoRaWAN SECURITY
LoRaWAN as a LPWAN protocol ensures low-power, low-cost, long-distance and secure communication for various IoT applications. According to the white paper published by the LoRa Alliance [23], LoRa’s communication range is longer than 15km. It uses unlicensed bands and a simple infrastructure to lower the cost for the construction of an IoT network. Security is a fundamental requirement for many IoT applications. The LoRaWAN security policy, which accords with state-of-the-art principles such as the use of a standard security algorithm and end-to-end secure communication protocols, enables mutual authentication, confidentiality and integrity. Therefore, the standardized AES cryptographic algorithm approved by the NIST (National Institute of Standards and Technology) is employed as the LoRaWAN security mechanism. It combines the original AES encryption/decryption algorithm with several modes of
operation, including a Cipher-based Message Authentication Code (CMAC) and a Counter Mode (CTR). The former is used to protect the integrity of messages, while the latter is employed for data encryption. When a new device joins, a unique 128-bit AppKey and a globally unique identifier DevEUI are utilized to generate application session key AppSKey and network session keys (NwkSKey for R1.0, and FNdSIntKey, SNwkSIntKey, NwKSEncKey for R1.1).

These session keys can be Activated By Personalisation (ABP) on the production line or during commissioning. It can also be Over-The-Air Activated (OTAA) in the field [10]. Figures 1 and 2 show how LoRaWAN traffic is protected using a NwkSKey and an AppSKey. Each payload encrypted by using an AES-CTR algorithm with an AppSKey carries a frame counter to protect the underlying system from replay attacks. A Message Integrity Code (MIC) computed by the AES-CMAC algorithm using the NwkSKey is verified by a network server to ensure packet integrity. When the content or header of a packet is compromised, and the network server cannot compute the correct MIC, the packet is dropped. Double-mode AES algorithms satisfy the security requirements in authentication and packet integrity for end nodes, network servers and application servers.

Although LoRaWAN reduces power consumption by using a well-defined communication mechanism and an efficient key generation process, the AES encryption (or decryption) process consumes much power of an end node, thus hard to ensure the 10-year battery life for a LoRaWAN [24].

B. AES OVERVIEW

In 2001, the NIST specified the Rijndael algorithm as an AES [16] to protect sensitive data. AES adopts symmetric block cipher scheme and supports the encryption/decryption key length in 128, 192, and 256 bits to meet different environmental needs. Depending on the key length, AES performs 10 to 14 encryption/decryption rounds, each of which (except the last round) consists of four steps, i.e., SubBytes, ShiftRows, MixColumns, and AddRoundKey, which are briefly described in the following.

- SubBytes: a nonlinear and invertible transformation. SubBytes often prepares a substitution table (i.e., SBox) or combinational logic to individually map bytes of a data array into other bytes. SBox entries are produced by calculating multiplicative inverses in a Galois Field by using an affine transformation.
- ShiftRows: byte transposition by rotating rows of the data array according to predefined offsets.
- MixColumns: multiplying each column of the data array by a modular polynomial equation or prime number in a Galois Field. Instead of computing separately, MixColumns can also be implemented by using large Lookup Tables.
- AddRoundKey: adding the data array with round-keys that are derived from an initial encryption key in the key expansion unit. This function XOR’s each byte of the data block with the corresponding byte in the round-key.

C. RELATED STUDIES

The mobile communication and IoT increase convenience for human beings’ lives. But they also presents many security challenges [25, 48]. Many studies seek to secure the IoT environment [24, 26, 27, 49]. Ning and Liu [26] proposed a cyber-physical-social-based security architecture to allow information security, physical security and management security. This security architecture supports the establishment of an information security model so as to secure different IoT environments. Li et al. [27] mentioned that, besides security, other aspects of IoT, including data confidentiality, integrity, availability and privacy, are also important. The study showed that multi-faceted security, such as user authentication, secure algorithm, access control and trust, is required for a modern IoT, especially in government and industry. Hui et al. [49] summarized the security challenges faced by IoT, including key management, intrusion detection, access control, and privacy protection. Besides, they also pointed out the advantages of applying blockchain technology to IoT.

Some studies [28-31] pointed out several weaknesses in LoRaWAN security. Grammatikis et al. [28] claimed that that key safety is essential. If one of two session keys is lost, a potential attacker can steal or tamper with a system’s important data. Butun et al. [50] analyzed the security risks of LoRaWAN by using ETSI guidelines and created a threat
catalog for LoRaWAN. They claimed that the threats, e.g., end-device physical capture, rogue gateways, and self-replay, damage the security of LoRaWAN-based IoT environment. Miller [29] imagined possible attacks on a LoRaWAN, and recommended that the session key management policy and the session key generation process need to be improved. The study also presented that a comprehensive message verification and key protection policy is required by all end nodes, concentrators/gateways and application servers in a LoRaWAN. In [30], Aras et al. demonstrated a LoRaWAN’s vulnerability using a physical equipment, demonstrating that a LoRaWAN packet does not contain time information. It is relatively easier for hackers to initiate replay attacks. Reynders et al. [31] also indicated that DoS attacks congest networks. This may occur during data transmission in a LoRaWAN when different network connections are allocated the same frequency.

Energy consumption is an important aspect when constructing an IoT network. Trappe et al. [32] presented that modern cryptography cannot secure the end nodes because the operating energy and computational capability are not conducive to traditional security approaches. Hung and Hsu [22] studied the power consumption and cryptographic calculation requirement for three different AES types given different payload lengths. The study showed that a hardware-based AES performs better than a software-based AES does, in terms of power consumption and computational latency.

Many low-power AES architectures and methods have been proposed in the recent decade. Hamalainen et al. [33] designed a compact 8-bit AES core that repeatedly computes a portion of the AES encryption to reduce power consumption and minimize circuit area. El-meligy et al. [34] used an asynchronous AES core, and Dao et al. [35] utilized a shared S-Box and a low switching activity shift-row operation to reduce energy consumption of AES data encryption. Shreedhar et al. [51] implemented a low gate-count ultra-small area AES for small-area applications. They reused the critical circuits, cascaded the input data, and minimized ShiftRow operation to reduce the AES gate counts so that the energy consumption can also be reduced. Bui et al. [36] optimized the AES by reorganizing the data encryption path and minimizing activities in the path to lower the number of data registers and the amount of combinational logic required.

In order to improve the LoRaWAN’s security, several studies [37-39] proposed new methods for key management, data encryption, and session key updating/generation. However, most of them add complex operations or procedures, which significantly increase their systems’ power consumption. Generally, the end nodes of an IoT are often powered by energy-limited batteries. Maintaining a high security level often involves the use of high energy. Even though some studies minimized an end node’s power consumption [40, 41] by using various low power design methods, only few consider the balance between power consumption and security.

III. LOW POWER AES DATA ENCRYPTION ARCHITECTURE (LPADA)

In the LoRaWAN specification, the AES encryption algorithm is used to encrypt data and to validate message integrity. To provide a low-power AES encryption circuit for the LoRaWAN environment, the LPADA utilizes an ultra-low-power Content Addressable Memory (CAM) for the SBox. Power gating and dynamic power management technologies are also adopted by the LPADA to reduce AES circuit’s dynamic and static power consumption. The LoRaWAN has two AES modes, i.e., CMAC and CTR, meaning that the proposed LPADA is an AES cryptography system with these two modes.

A. DATA ENCRYPTION ARCHITECTURE

To implement an AES on a LoRaWAN end node and to minimize the power consumed by the AES encryption process, the LPADA constructs several functional blocks. As shown in Figure 3, not only the aforementioned AddRoundKey, SubBytes, MixColumns and ShiftRows functional blocks are implemented, but also the Key Expansion block is designed to expand the original encryption key into a number of round keys. At the beginning of the AES encryption process, one of the AppSKey and NwkSKey is selected by the M1 multiplexer as the encryption key. In the first round of the AES process, the plaintext and the selected encryption key are respectively chosen by the M2 multiplexer and the M3 multiplexer as the inputs for the AddRoundKey function block. The SubBytes, MixColumns and ShiftRows functions are then operated in sequence. After the first round, the output and round key are both used in the next round. After 10 rounds, the M4 demultiplexer outputs the ciphertext.

In Figure 3, according to the contents of the SBox, SubBytes block transforms an input into an output value. A low power CAM is utilized to reduce the power consumption of SBox. The details of this process are given in the following section. A Power Management Unit is also adopted to block/unblock clock signals and supply voltages to each functional block. When the circuit is not in use, its
clock/supply voltage is gated to mitigate dynamic and static power consumption. However, the Power Management Unit and SBox are unaffected when other functional blocks’ clock/voltage are gated, so their functionality and content are maintained.

B. SBox DESIGN

In the AES architecture, the SBox individually maps bytes of a data block into other bytes during the SubBytes step. SBox can be implemented by using two methods: combinational circuits and a lookup table in memory. The former consumes less power than the memory does but it has a longer computational latency. CAM allows fast data searching due to the feature of parallel searching.

However, CAM consumes much power because all of the search-lines and match-lines in the CAM cells must be initialized before data search. It means all search-lines are set to GND and all match-lines are pre-charged to VDD so as to prevent the short-circuit current in the match-lines passing through the pull-down paths. At the beginning of evaluation phase, depending on the search data, some search-lines are charged to VDD and the CAM cells then compare their stored data with the search-lines’ values. The match-line for a specific CAM entry is discharged to GND when one or more CAM cells in this CAM entry are mismatched. Only when all CAM cells in a specific CAM entry are matched, the match-line of that CAM entry can keep its voltage as VDD in the initial phase. In the LPADA, a low power CAM architecture [42] from a previous study by the authors is used to implement SBox. The low power CAM utilizes an automatic charge balancing mechanism which is developed based on the complementary features of the N-type CAM and the P-type CAM.

C. POWER GATING

Power gating switches off supply voltage or blocks discharging-path so that the electric current cannot pass through the transistors, and thus the dynamic and static power consumptions of those gated blocks can be reduced. There are two common categories of power gating techniques: those that use a PMOS to turn off the power supply and those that use a NMOS to turn off the ground path. If a PMOS is used, then when the circuit operates, the PMOS is turned on and the external current enters the main circuit. Otherwise, the PMOS is turned off so the entire circuit is switched off. In the LAPDA, PMOS-based supply power gating is used for the entire AES circuits, except the SBox memory, which requires power to maintain its data.

D. POWER MANAGEMENT

For dynamic power management (DPM), the supply voltage and the clock frequency of some components are dynamically changed during these components’ execution period. Generally, when some functional blocks do not operate at high-speed, DPM reduces or turns off the operating voltage/clock frequency to lower dynamic power consumption and static power consumption. As shown in Figure 4, in a LPADA the AES architecture has three operational modes: the active mode, the idle mode and the sleep mode. Initially, the LPADA is in idle mode. When it receives an action request to encrypt or decrypt data, the LPADA enters the active mode. When data encryption/decryption is complete, the LPADA returns to idle mode and waits for the timer T_{IS}’ s trigger, where T_{IS} is a user-defined period of time. In this study, the T_{IS} value is 5 minutes. When the LPADA is triggered by T_{IS}, it switches to sleep mode. The power control policies for the three modes are as follows.

- Active mode: no power gating nor clock gating for functional blocks.
- Idle mode: clocks for all sequential circuits are gated to reduce dynamic power consumption.
- Sleep mode: supply voltages for all circuits, except SBox and key registers, are gated.

Three power modes are used for a power management policy to represent active, idle and sleeping status. In some systems, the sleeping mode comprises a light sleeping mode and a deep sleeping mode. However, the greater the number of power modes are used in the circuit design, the more complex control circuits are required in an end node. That is to say that a high circuit area overhead and high-power-consumed control circuit are necessary. For a battery-powered end node, a high-power consumption control circuit negates the benefit of a power management policy, so this study uses only three basic power modes to balance power consumption and circuit complexity.

E. SESSION KEY UPDATE PROCEDURE

According to the LoRaWAN specification [10], the session keys are updated by using the rejoin procedure. However, the key management policy is not well defined by this specification [43, 44] and the rejoin procedure gives no forward secrecy, so the LoRaWAN is susceptible to suffer attacks. The LPADA uses a key update procedure developed in our previous study [45]. As shown in Figure 5, where EN represents an end node, JS means join server, and NS and AS represent a network server and an application server, respectively. There are three steps in the key updating procedure.
ADA and traditional aes, increasing rapidly in deep.

KeyUpdateReq

FIGURE 5. Session key update procedure.

Step 1: the EN sends a key update request message, KeyUpdateReq, to JS, where

KeyUpdateReq = aes128_encrypt(LastAppSKey@NwkKey, 0x02 | Random | Hash(JoinNonce|DevEUI|Random))

in which aes128_encrypt means that the AES encryption process is used for message encryption with encryption key length of 128 bits, LastAppSKey is the previous AppSKey, NwkKey is one of root keys stored in both EN and JS, Random is a random number generated by EN, Hash is a one-way hash function, JoinNonce is a lifetime counter that calculates the number of join times and DevEUI is the unique identification number of EN.

Step 2: when JS receives KeyUpdateReq sent by EN, it generates a new AppSKey and a new NwkSKey by using LastAppSKey, Random, and the previous network session key, LastNwkSKey where

AppSKey = aes128_encrypt(LastAppSKey@Random, 0x02 | Hash(JoinNonce|Random|DevEUI))

NwkSKey = aes128_encrypt(LastNwkSKey@Random, 0x01 | Hash(JoinNonce|NetID|Random|DevEUI))

The answer to the key updating request KeyUpdateAns is also calculated and then delivered to EN where

KeyUpdateAns = aes128_encrypt(AppSKey@NwkKey, 0x02 | Hash(Random|KeyUpdateReq))

Step 3: when EN receives the answer of key updating request, it decrypts the message and verifies received Hash(KeyUpdateReq). If the message passes the verification, EN calculates a new AppSKey and a new NwkSKey with the same method as JS in Step 2, and generates an acknowledgement message KeyUpdateAck which is then sent to the JS where

KeyUpdateAck = aes128_encrypt(AppSKey@NwkSKey, 0x02 | JoinEUI|DevEUI)

When the JS receives KeyUpdateAck, it verifies this acknowledgement message and respectively delivers new AppSKey and NwkSKey to the application server and network server when the KeyUpdateAck passes the verification.

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

A. IMPLEMENTATION ENVIRONMENT

To verify the feasibility and power consumption of the LPADA, Verilog HDL is utilized to implement the AES circuit which is then synthesized with Synopsys Design Compiler and Synopsys 32nm cell library. Design Compiler, a popular logic synthesis tool developed by Synopsys Inc., optimizes the circuit design to provide the smallest and fastest logical representation of a given function. In the LPADA, voltages of 0.7v, 0.75v, 0.85v, 0.95v and 1.05v are used to estimate the circuit’s power consumption at a temperature of 25°C. Figure 6 shows the circuit diagram of the LPADA.

B. EXPERIMENTAL RESULTS

The dynamic power, static power and latency of the LPADA and a traditional AES architecture are shown in TABLE I, in which “Trad.” represents a traditional AES architecture and “R%” indicates the reduction percentage defined as (Trad. – LPADA)/Trad. Since power consumption is directly proportional to operating voltage. TABLE I shows that when the circuit operates at 0.7v, both the LPADA and traditional AES architecture have the lowest dynamic power consumption and static power consumption. However, lower voltages also result in a longer computational latency. On average, the LPADA reduces 62.0% of dynamic power consumption, 88.5% of static power, and -38.8% of computational latency compared to a traditional AES architecture. This table also illustrates that for both the LPADA and the traditional AES, the dynamic power is much smaller than the static power because the leakage current increases rapidly in deep-submicron design technology.

Since power gating is used in the LPADA to turn off the supply voltage of those temporarily unused functional blocks and a low-leakage CAM is also employed to implement SBox, the static power consumption of the LPADA is much smaller than that of a traditional AES architecture.

C. CASE STUDY: END NODE ENERGY CONSUMPTION FOR DATA UPLINK

When an end node sends data to an application server, the data must be packed in a MAC message, as shown in Figure 7, in which PHDR represents the LoRa physical header,
PHDR_CRC is the cyclic redundancy check (CRC) code of the physical header. PHYPayload means the physical payload and last CRC is added to protect whole message’s integrity. The PHYPayload can be further divided into a MAC header (MHDR), a MAC payload (MACPayload), and a message integrity code (MIC). The MACPayload of the data message contains a frame header (FHDR), followed by a port field (FPort) and a frame payload field (FRMPayload).

In the LoRaWAN, the security and integrity of the data is protected in the MAC layer; that is to say that both MACPayload and MIC perform AES encryption procedures. The FRMPayload field should be encrypted before the MIC is calculated. In order to encrypt FRMPayload, for each data message, LoRa defines a sequence of blocks, $A_i$, for $i = 1 \ldots k$ with $k = \lceil \text{length}(\text{FRMPayload})/16 \rceil$, where $\text{FRMPayload}$ is the encrypted field. Not only data, but each $A_i$ also includes the end node address $\text{DevAddr}$, and a counter $\text{FCntUP}$ used to monitor the number of data frames that are uplinked to the network server. Blocks $A_i$ are then encrypted to give a sequence $S$ of blocks $S_i$ as

$$S = \text{aes128}_{\text{encrypted}}(\text{AppSKey}, A_i)$$

The payload is then encrypted by truncating $(\text{pld}/16) \times r$ to the first $\text{length}(\text{pld})$ octets. The MIC field is also calculated using the AES as:

$$\text{cmacS} = \text{aes128}_{\text{cmac}}(\text{SNwkSIntKey}, B_j[\text{MHDR}]\text{MACPayload})$$

$$\text{cmacF} = \text{aes128}_{\text{cmac}}(\text{FNwkSIntKey}, B_0[\text{MHDR}]\text{MACPayload})$$

$$\text{MIC} = \text{cmacS}|\text{cmacF}$$

In cmacS and cmacF, the SNwkSIntKey and FNwkSIntKey are the network session keys for the serving network server and the forwarding network server, respectively. $B_j$ and $B_0$ are two information blocks that contain information about the device address, the uplink counter and the message length.

### Table I

<table>
<thead>
<tr>
<th>Operating Voltage</th>
<th>Dynamic Power (µW)</th>
<th>Static Power (µW)</th>
<th>Latency (ns)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LPADA</td>
<td>Trad.</td>
<td>R%</td>
</tr>
<tr>
<td>0.7v</td>
<td>149.28</td>
<td>275.24</td>
<td>45.8%</td>
</tr>
<tr>
<td>0.75v</td>
<td>150.48</td>
<td>307.88</td>
<td>51.1%</td>
</tr>
<tr>
<td>0.85v</td>
<td>152.73</td>
<td>365.20</td>
<td>56.0%</td>
</tr>
<tr>
<td>0.95v</td>
<td>159.46</td>
<td>492.40</td>
<td>68.5%</td>
</tr>
<tr>
<td>1.05v</td>
<td>167.54</td>
<td>552.43</td>
<td>71.5%</td>
</tr>
<tr>
<td>Average</td>
<td>153.02</td>
<td>402.63</td>
<td>62.0%</td>
</tr>
</tbody>
</table>

### Figure 7

MAC message format for LoRaWAN data uplink.

### Figure 8

Energy consumption comparison between the LPADA and traditional AES architecture under different message payload lengths.

In summary, $k+2$ AES encryptions are required to send a message from one end node to a network server when the payload is smaller than the predefined maximum payload. Without considering static power consumption, Figure 8 shows the transmission of uplink data for different message lengths. The figure shows that the LPADA consumes less energy than a traditional AES architecture, especially when the message payload is long.

## V. SECURITY ANALYSIS AND DISCUSSIONS

In this paper, since the original AES with CMAC and CTR modes are used, the security of the LPADA is the same with AES original version. The security analysis of AES algorithm can be seen in [46, 47]. The security analysis for key update procedure is as follows.

### A. SECURITY ANALYSIS FOR KEY UPDATE PROCEDURE

1) Mutual authentication

Mutual authentication guarantees that only an authentic EN can perform the key updating procedure with a genuine JS. In a LoRaWAN, an authentic EN and a genuine JS have the original root keys: AppKey and NwkKey. Therefore, without the necessary correct root keys, fake EDs or servers cannot complete the key updating procedure. In Step 1 of the key updating procedure, EN generates a random number, $\text{Random}$, which is encrypted using $\text{LastAppSKey}$ and $\text{NwkKey}$, and then sent to JS. A hash value is also calculated, encrypted, and sent to JS. In Step 2, the JS calculates the hash value by using the information conveyed in the decrypted message, and then compares the hash...
value with received hash value to verify EN’s identification. An answer message, KeyUpdateAns, which includes Random and KeyUpdateReq, is encrypted using a new AppSKey and the original NwkKey. In Step 3, EN decrypts KeyUpdateAns and verifies the hash value. If the hash value is verified, the mutual authentication is confirmed.

(2) Replay attack resistance

In the LoRaWAN, JoinNonce is a lifetime counter that calculates the number of join times. Since this counter is managed and stored by EN and JS, when a hacker captures and duplicates a valid message and then retransmits this message to JS, the JoinNonce value of the retransmitted message must be different with the one held by EN and JS. This means that the received message is not from a genuine EN, so this counter can be used to resist a replay attack.

(3) Eavesdropping attack resistance

When a hacker captures a large number of messages from the underlying network, sensitive information might be extracted. In each step of the LPADA key update procedure, the important messages are encrypted using a combination of two of five keys, including LastAppSKey, NwkKey, Random, AppSKey and NwkSKey. Since Random is generated in step 1 of each key update procedure, and it is also a temporal value only used in one time of the key updating procedure, a new AppSKey and a new NwkSKey are calculated by using this random number. As a result, the hacker cannot access important information by using accumulated messages.

B. DISCUSSIONS

In this paper, the LPADA is proposed to reduce the LoRaWAN end nodes’ encryption and decryption power without changing the encryption mechanism. The experimental results in Section 4.2 show that dynamic power consumption is reduced by 62% and static power consumption by 88.5%, compared to those of a traditional AES architecture. Therefore, we can conclude that the LPADA does improve the power consumption. However, the LPADA also causes a decrease in performance because the LPADA uses a serial architecture to encrypt/decrypt data, so several rounds are required to encrypt/decrypt one data block. Power gating and power management often turn off the supply power and system clock in temporarily unused functional blocks and turns on them when an action request is received. However, the turn-on/turn-off action requires an additional control circuit, which increases the latency time. In many IoT applications, a small amount of infrequently transmitted data is often generated. Therefore, low power consumption is much more important than performance.

VI. CONCLUSION AND FUTURE STUDIES

To reduce power consumed by LoRaWAN’s end nodes in a secure data encryption architecture, the LPADA is proposed in this study. Three low-power design technologies are implemented in the LPADA, including a low-power CAM for SBox, power gating to gate the functional blocks’ supply voltages and power management to control the functional blocks’ power states. Both dynamic power consumption and static power consumption are reduced using the proposed AES architecture. The power-delay-product also demonstrates that the LPADA is relatively suitable for IoT. The security analyses show that the key updating procedure enables mutual authentication and resists a replay attack and an eavesdropping attack.

Future study will involve the functions of the AES circuit being performed in parallel and the use of more low-power design technologies for the LPADA to reduce power consumption and decrease encryption/decryption delays. The AES architecture’s formal power model will also be studied.

ACKNOWLEDGMENT

The authors would also like to express thanks to Synopsys Inc. and Dr. Charles Chiang of Synopsys Inc. for donation of “Tunghai University Design Automation Education” project to enhance the education of electronic design in Tunghai University. Besides, the authors would like to acknowledge software and cell library support provided by Taiwan Semiconductor Research Institute (TSRI), Taiwan, R.O.C.

REFERENCES


