密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2021, 8(5): 834–843

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

AES-CCM 通用协处理器的优化设计实现*

崔 超, 赵 云, 肖 勇, 林伟斌, 曾勇刚

南方电网科学研究院有限责任公司, 广州 510663
通信作者: 崔超, E-mail: cuichao2020@163.com

摘 要: 为了减小 AES-CCM 加密协议的电路面积和功耗, 本文利用 AES-CCM 链路层数据加密与解密都只用到 AES 加密模式, 以及数据校验值生成与数据加解密可以同时计算且密钥相同的特点, 给出 AES-CCM 通用协处理器的一种低功耗实现方案. 该方案以 AES 加密模块为运算核心, 在外围 CCM 模块的协同控制下实现 AES-CCM 加密协议. 其中, 外围 CCM 控制模块固定不变, AES 加密模块可根据不同的应用需求进行选择性例化: 面向高速率指标的产品实现时选择 AES 双轮并行实现方式, 面向低代价指标的产品实现时选择 AES 双轮乒乓实现方式. 与传统双 AES 并行实现的 AES-CCM 方案相比, AES 双轮并行实现 AES-CCM 方案的面积和功耗分别减小 9.21% 和 12.34%; 与传统双 AES 串行实现的 AES-CCM 方案相比, AES 双轮乒乓实现 AES-CCM 方案的面积增加 0.06%, 但是功耗减小 12.12%.

关键词: AES-CCM; 数据认证; 加密; 低功耗

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000480

中文引用格式: 崔超, 赵云, 肖勇, 林伟斌, 曾勇刚. AES-CCM 通用协处理器的优化设计实现[J]. 密码学报, 2021, 8(5): 834–843. [DOI: 10.13868/j.cnki.jcr.000480]

英文引用格式: CUI C, ZHAO Y, XIAO Y, LIN W B, ZENG Y G. Optimal implementation of AES-CCM general coprocessor[J]. Journal of Cryptologic Research, 2021, 8(5): 834–843. [DOI: 10.13868/j.cnki.jcr.000480]

Optimal Implementation of AES-CCM General Coprocessor

CUI Chao, ZHAO Yun, XIAO Yong, LIN Wei-Bin, ZENG Yong-Gang

Electric Power Research Institute of CSG, Guangzhou 510663, China
Corresponding author: CUI Chao, E-mail: cuichao2020@163.com

Abstract: In order to reduce the circuit area and power consumption of AES-CCM encryption protocol, using the characters of AES-CCM link layer data encryption and decryption based on AES encryption algorithm, data check value generation and data encryption and decryption can be calculated at the same time and with the same key, this paper presents a low-power implementation scheme of AES-CCM general coprocessor. The AES-CCM encryption protocol is implemented under the cooperative control of peripheral CCM modules with AES encryption module as the core. The peripheral CCM control module is fixed and the AES encryption module is selectively instantiated according to different application requirements: AES double wheel parallel implementation is selected for high-speed target-oriented product implementation, and AES double wheel ping-pang implementation

* 基金项目: 自主高安全计量用电安全芯片关键技术研究 (ZBKJXM20180014/SEPRI-K185011973)
Foundation: Research Project on Key Technologies of Independent High Safety Metering Power Safety Chip (ZBKJXM20180014/SEPRI-K185011973)
收稿日期: 2020-11-12 定稿日期: 2020-12-11

is selected for low-cost target-oriented product implementation. Compared with the traditional double AES parallel implementation of AES-CCM scheme, the area and power consumption of AES-CCM scheme with two parallel wheels of AES are reduced by 9.21% and 12.34% respectively; compared with the traditional double AES serial implementation of AES-CCM, the area of AES-CCM scheme with two ping-pang wheels of AES is increased by 0.06%, however, the power consumption is reduced by 12.12%.

Key words: AES-CCM; authentication; encryption; low-cost

1 引言

AES-CCM (advanced encryption standard-cipher block chaining and counter mode) 加密协议作为无线局域网安全标准, 由 IEEE 无线标准小组于 2004 年公布 [1], 同时具备验证无线通信中链路层数据完整性、真实性和保障数据安全性的功能, 目前已广泛被 802.11、802.15、802.16、Bluetooth、Zigbee 等无线通讯协议采用.

基于 AES-CCM 加密协议在智能家居、可穿戴设备、智能驾驶等无线终端设备的广泛应用需求, AES-CCM 加密协议的实现方式逐渐成为研究热点. 目前在工业领域, AES-CCM 加密协议普遍采用 CCM 分组模式软件实现、AES 加密核硬件实现的方式, 该方式实现简单灵活, 但是运算时产生的取指令、指令译码等操作占用本来就有限的 CPU 内存资源, 从而影响数据处理速度和系统功耗. 在研究领域 Nguyen 等人将 CBC (cipher block chaining mode) 和 CTR (counter mode) 并行计算, 提出了双 AES 加密核的硬件高吞吐率实现方式, 在 269 MHz 的最高频率下, 吞吐率能达到 2.69 Gbps [2]; Pammu 等人提出 9-core 并行方案 [3], 在数据加密时多路并行计算, 在校验值生成时, 利用有限域 GF(2^8) 上的乘法将每 16×128 比特转换为 128 比特再送进 CBC 模块计算校验值, 将数据处理速率提高至 8.32 Gbps. 以上研究大多是为了提高了数据吞吐率, 而在实际应用中如 BLE 产品、Zigbee 产品等, 有时候不需要太高的数据吞吐率, 更关注产品的面积和功耗指标. 因此, 有必要对 AES-CCM 加密协议的低代价实现进行研究.

本文给出 AES-CCM 通用协处理器的低功耗实现方案, 该方案将传统方法中粗粒度的双 AES 并行或双 AES 串行实现 [4,5] 细化为共享轮密钥的双轮并行或双轮乒乓方式, 如此能够在保证吞吐率一致的前提下, 减少冗余电路的实现和计算, 从而降低面积和功耗的开销.

本文结构如下: 第 2 节介绍了 AES-CCM 加密协议; 第 3 节对 AES-CCM 通用协处理器的 CCM 控制模块以及 AES 加密模块的双轮并行和双轮乒乓实现方案进行阐述; 第 4 节介绍仿真综合结果; 第 5 节对方案进行总结.

2 AES-CCM 加密协议

AES-CCM 协议的核心加密模块主要由 AES 算法构成, 外围控制模块由经典的密文块连接 CBC 分组模式和计数器 CTR 分组模式构成, 其结构如图 1 所示.

CBC 分组模式主要用于压缩数据生成消息完整性校验值 (message authentication code, MAC), 数据发送前, 发送方对明文数据压缩, 生成消息验证码 MAC 值附于明文后, 发送给接收方. 接收方收到数据后用同样的 CBC 分组模式压缩明文得到另一个 MAC 值, 并将两个 MAC 值比较, 若一致, 则接收数据无误, 以此来验证数据的完整性和真实性. CBC 分组模式中 AES 的输入为包含数据包头、数据长度、数据明文等信息的特定分组与前一组 AES 密文输出 Y_{i-1} 的异或值. 其计算过程如下, 其中 B_0、B_1 为包含数据包头和数据长度的 128 比特数据, P_i 为 128 比特的明文分组.

$$
\begin{aligned}
Y_0 &= \mathrm{En}_{\mathrm{key}}(B_0)\\
Y_1 &= \mathrm{En}_{\mathrm{key}}(Y_0 \oplus B_1)\\
Y_2 &= \mathrm{En}_{\mathrm{key}}(Y_1 \oplus P_1)
\end{aligned}
$$

$$\vdots$$
$$Y_{n+2} = \mathrm{En}_{\mathrm{key}}(Y_{n+1} \oplus P_{n+1})$$
$$\mathrm{MAC} = \mathrm{MSB}(Y_{n+2})$$

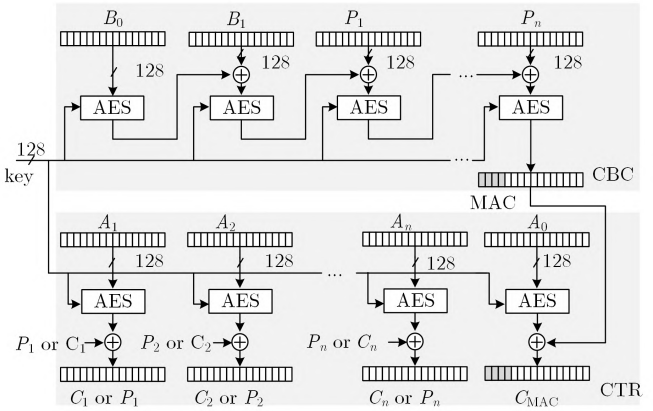

图 1 AES-CCM 结构图
Figure 1 Structure diagram of AES-CCM

CTR 分组模式主要用于对传输数据加解密. 发送方将明文数据和 MAC 值拼接起来并分成等长度的数据组, 每组与计数器加密结果进行异或操作得到该组密文, 接收方接到密文数据后用同样的方法将密文分组分别与计数器的加密结果异或得到明文分组以及传输的 MAC 值. 该分组模式的加密流程和解密流程完全一样. AES 的输入为包含数据组计数值信息的数据 A_i, AES 的密钥 key 同生成校验值使用的密钥 key 相同, 其计算过程如下:

$$C_1 = \mathrm{En}_{\mathrm{key}}(A_1) \oplus P_1 \text{ or } P_1 = \mathrm{En}_{\mathrm{key}}(A_1) \oplus C_1$$
$$C_2 = \mathrm{En}_{\mathrm{key}}(A_2) \oplus P_2 \text{ or } P_2 = \mathrm{En}_{\mathrm{key}}(A_2) \oplus C_2$$
$$\vdots$$
$$C_n = \mathrm{En}_{\mathrm{key}}(A_n) \oplus P_n \text{ or } P_n = \mathrm{En}_{\mathrm{key}}(A_n) \oplus C_n$$
$$C_{\mathrm{MAC}} = \mathrm{MSB}(\mathrm{En}_{\mathrm{key}}(A_n)) \oplus \mathrm{MAC})$$

传统的 AES-CCM 加密协议的全硬件实现技术有两种: 两个 AES 加密核并行实现方案和一个 AES 加密核串行实现方案, 分别如图 2 中左右所示. AES-CCM 加密协议并行实行实现方案采用两个 AES 加密核并行分别实现 CBC 分组模式和 CTR 分组模式. CTR、CBC 加密模式中被加密的明文互不相同, 都由几块数据组成, 所以需要 Ai_gen 和 Bi_gen 模块按不同的阶段产生 CTR 所需的 A_i 和 CBC 所需的 B_i, 分别输入到两个 AES 加密核中.

AES-CCM 加密协议串行实现方案采用一个 AES 加密核串行实现, 以时分复用的方式分别完成 CBC 和 CTR 分组模式的计算. A_i 和 B_i 在 CTRL 模块的控制下, 交替输入到 AES 加密核中.

3 AES-CCM 通用协处理器的优化设计

对 AES-CCM 加密协议进行分析, 如图 3 所示, 当设备作为数据发送方时:

(1) CBC 模式比 CTR 模式多计算一组数据 B_0;

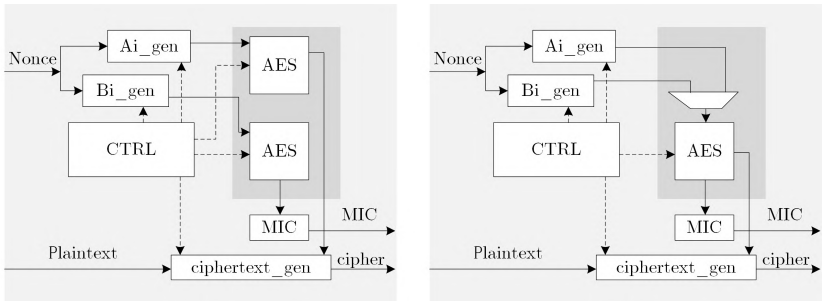

图 2　传统 AES 并行实现 AES-CCM 方案 (左) 传统 AES 串行实现 AES-CCM 方案 (右)

Figure 2　Traditional parallel implementation (left) and traditional serial implementation of AES-CCM (right)

(2) $B_1 \oplus Y_0$ 与 A_1 的数据加密可以同步执行;

(3) 当获取到 128 比特明文数据 P_1 且 AES 加密完成后, P_1 可以与 A_1 的加密结果异或得到密文 C_1, 继而 $P_1 \oplus Y_1$ 和 A_2 数据加密可以同步执行;

(4) 当获取到明文 P_2 且 AES 加密完成后, P_2 可以与 A_2 的加密结果异或得到密文 C_2, 继而 $P_2 \oplus Y_2$ 和 A_3 数据加密仍然可以同步执行;

(5) 以此类推, 直到处理完所有明文数据.

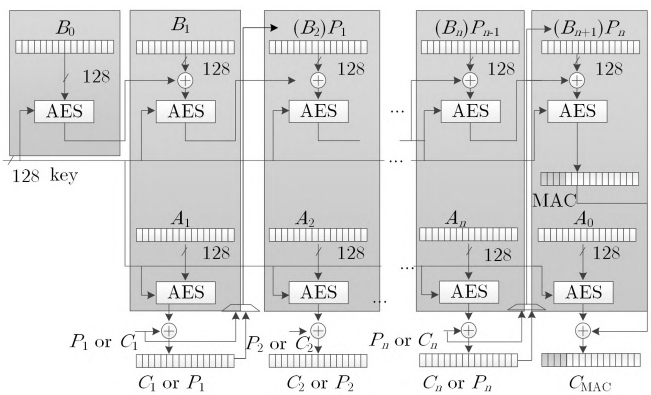

图 3　AES-CCM 数据处理结构图

Figure 3　AES-CCM data processing structure diagram

因此除了 B_0 的 AES 加密运算可以单独执行外, 其他所有数据分组 CBC 和 CTR 的 AES 加密运算都可以同步执行.

当设备作为数据接收方时,

(1) 同样 CBC 模式比 CTR 模式多计算一组数据 B_0;

(2) $B_1 \oplus Y_0$ 与 A_1 的数据加密可以同步执行;

(3) 当接收到 128 比特密文数据 C_1 且 AES 加密完成后, C_1 可以与 A_1 的加密结果异或得到明文 P_1, 继而 $P_1 \oplus Y_1$ 和 A_2 数据加密可以同步执行;

(4) 当接收到密文 C_2 且 AES 加密完成后, C_2 可以与 A_2 的加密结果异或得到明文 P_2, 继而 $P_2 \oplus Y_2$ 和 A_3 数据加密仍然可以同步执行;

(5) 以此类推, 直到处理完所有密文数据.

因此除了 B_0 的 AES 加密运算可以单独执行外, 其他所有数据分组 CBC 和 CTR 的 AES 加密运算也都可以同步执行.

由以上分析, 归纳出 AES-CCM 加密协议的 3 个特点如下:

(1) 无论设备作为数据的发送方或者数据的接收方, AES-CCM 加密协议中仅用到 AES 的加密模式, 因此硬件实现中为减小设备的功耗和面积可以省去 AES 解密模式的实现.

(2) AES-CCM 加密协议中除了 CBC 模式第一组数据, 其他分组 CBC 模式和 CTR 模式的 AES 加密运算可以同步执行.

(3) AES 在 CBC 模式和 CTR 模式中所用到的密钥相同, 因此为减小功耗, 两个同步执行的 AES 计算可以在共享一个密钥扩展模块的方式下以两个轮函数并行实现的方式计算, 或以一个轮函数乒乓处理 CBC 模式和 CTR 模式数据的方式计算, 3.2 节与 3.3 节将给出并行实现和乒乓处理方式的具体过程.

根据以上 AES-CCM 加密协议的特点, 我们设计实现了 AES-CCM 通用协处理器, 外围控制模块与传统双 AES 并行和单 AES 串行实现方案一致, AES 加密模块根据具体的应用场景可以选择性实现. 在高吞吐率要求的应用场景选择 AES 加密模块双轮并行实现, 在低电路面积要求的应用场景选择 AES 加密模块双轮乒乓实现, 其电路结构如图 4 所示.

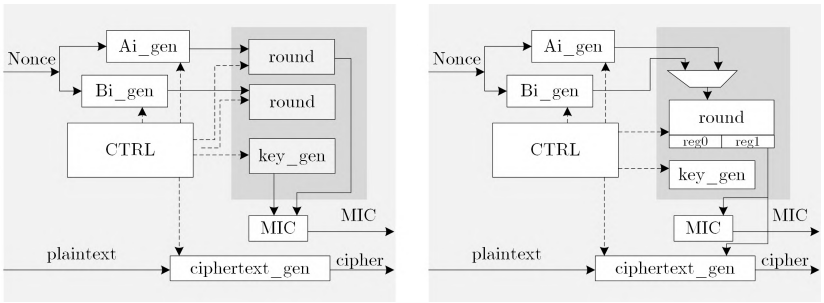

图 4 AES 双轮并行实现 AES-CCM 方案 (左) AES 双轮乒乓实现 AES-CCM 方案 (右)

Figure 4 Double wheel parallel (left) and double wheel ping-pang (right) implementation of AES-CCM

3.1 CCM 控制模块的实现

CCM 模块主要由状态机构成, 其状态跳转如图 5 所示. CCM 的控制过程如下:

(1) 在 IDLE 状态下 AES-CCM 模块的使能信号有效后, 执行第 (2) 步, 状态由 IDLE 状态跳转到 GET_B0 状态.

(2) 在 GET_B0 状态下, 获取数据 B_0, 数据准备好后, 执行第 (3) 步, 状态跳转到 AES_ENCODE_S 状态.

(3) 在 AES_ENCODE_S 状态下, 使能 AES 加密模块, AES 的加密模式配置为单数据组加密模式, 只执行 128 比特数据加密. AES 加密完成后, 执行第 (4) 步, 状态跳转到 GET_BX_AX 状态.

(4) 在 GET_BX_AX 状态下, 获取数据 $B_x(P_{x-1})$、A_x, 数据准备好后, 执行第 (5) 步, 状态跳转到 AES_ENCODE_D 状态.

(5) 在 AES_ENCODE_D 状态下, 使能 AES 加密模块, AES 的加密模式配置为双数据组加密模式, 执行 2×128 比特数据加密. AES 加密完成后, 若当前数据组不是最后一组数据, 则执行第 (4) 步, 状态跳转回 GET_BX_AX 状态, 获取下一组数据; 若当前数据组是最后一组数据, 则执行第 (6) 步, 状态跳转到 GET_PN_A0 状态, 进行 P_n 和 A_0 数据获取; 若当前数据组为 MAC 标志的数据组, 表示所有待加密数据组均完成加密, CBC 模式的加密输出生成 MAC 值, CTR 模式的加密输出异或 MAC 值, 以完成对 MAC 值的加密, 至此 AES-CCM 的所有数据处理完成, 状态跳转回 IDLE 状态, 等待下一次 AES-CCM 的使能.

(6) 在 GET_PN_A0 状态下, 获取数据 P_n 和 A_0, 当 P_n 和 A_0 数据准备好后, 则执行第 (5) 步, 状态跳转回 AES_ENCODE_D 状态.

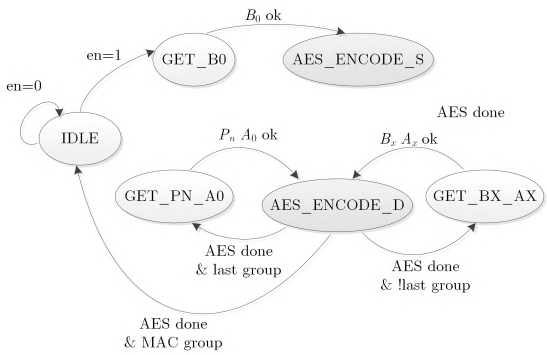

图 5　CCM 控制模块的状态机

Figure 5　Finite state machine of CCM control module

3.2　AES 加密模块双轮并行实现

CCM 状态机执行数据加密的状态只有 AES_ENCODE_S 状态和 AES_ENCODE_D 状态, AES_ENCODE_S 状态完成 128 比特数据加密, 每次启动 AES-CCM 加密协议, 该状态只执行一次. AES_ENCODE_D 状态完成 2×128 比特数据加密, 每次启动 AES-CCM 加密协议, 该状态根据数据包的长度多次重复执行, 因此 AES_ENCODE_D 状态下的加密操作可以设计成两个 AES 并行执行或串行执行的方式, 同时, 由于 CBC 模式和 CTR 模式所使用的密钥相同, 为了减少功耗和电路面积, 可以共享密钥扩展模块, 以轮并行和轮乒乓串行的方式替代两个 AES 并行执行或串行执行的方式完成 2×128 比特数据加密.

AES 加密模块双轮并行实现的电路结构如图 6 所示, 由两个轮迭代模块和一个密钥扩展模块构成. 密钥扩展模块完成轮密钥的扩展, 并共享给两个轮迭代模块使用, 轮迭代 Core_0 和轮迭代 Core_1 分别完成两组数据的的轮迭代加密. 两个轮迭代模块的使能信号单独控制, 当只需要加密 128 比特数据时, 只使能一个轮迭代模块, 另一个轮迭代模块停止工作, 以减小系统功耗; 当并行加密 2×128 比特数据时, 使能信号 en[0], en[1] 都有效, 并行加密两组数据.

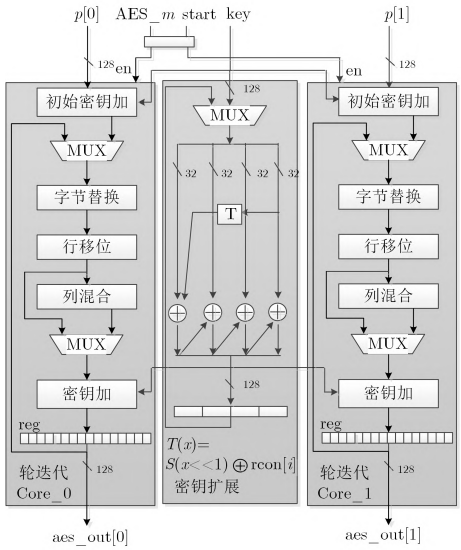

图 6　AES 双轮并行实现电路结构

Figure 6　Circuit structure of AES double wheel parallel implementation

将该方案与传统双 AES 并行方案对比分析, 我们发现, 该方案减少了一个密钥扩展模块的电路实现和计算, 从而减小了整体能耗和电路面积.

3.3 AES 加密模块双轮乒乓实现

AES 加密模块双轮乒乓实现的电路结构如图 7 所示, 由一个轮迭代模块和一个密钥扩展模块构成. 当执行 128 比特数据加密时, AES 配置成单数据组加密模式, 完成一次 128 比特数据加密需要 10 个周期, 每个周期完成一次密钥扩展和一次轮迭代计算轮迭代模块的输出寄存器只用到 reg_0, reg_1 保持不变; 当执行 2×128 比特数据加密时, AES 配置成双数据组加密模式, 完成 2×128 比特数据加密需要 20 个周期, 每一轮函数计算由两个周期完成, 周期 1 完成当前轮的密钥扩展和数据组 0 的轮迭代, 并将轮迭代结果寄存至 reg_0, 周期 2 不需要执行密钥扩展, 只完成数据组 1 的轮迭代, 并将轮迭代结果寄存至 reg_1.

将该方案与传统双 AES 串行方案对比分析, 我们发现, 完成 2×128 比特数据加密, 该方案减少了 10 次密钥扩展的计算, 从而减小了整体能耗, 但是电路代价为多一组 128 比特的寄存器.

此外, 以上两种 AES 加密方案在轮迭代模块和密钥扩展模块的 S 盒实现时利用了同构映射, 将复合域 $\mathrm{GF}(2^8)$ 上的求逆运算映射到 $\mathrm{GF}(((2^2)^2)^2)$ 上 [6–8], 并对 $\mathrm{GF}((2^2)^2)$ 域上的逻辑表达式以及相邻变换的表达式结合化简, 进一步降低功耗, 缩小关键路径的延时.

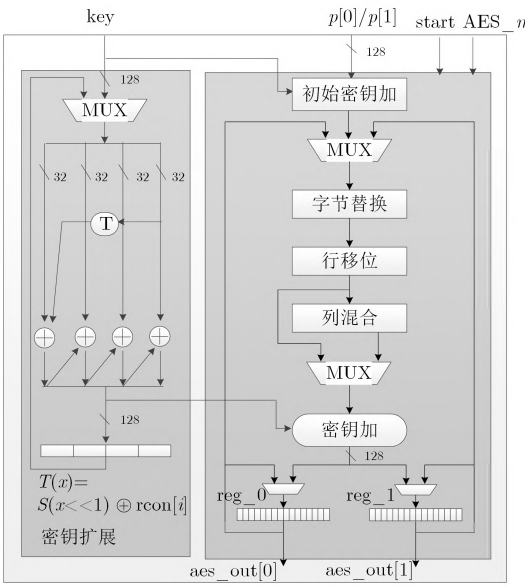

图 7 AES 双轮乒乓实现电路结构

Figure 7 Circuit structure of AES double wheel ping-pang implementation

4 仿真综合验证

为了对方案的功能进行验证, 我们对方案进行 RTL 代码实现, 利用 VCS 仿真软件结合 Testbench 验证脚本和测试激励, 完成各模块的功能验证.

AES 的加密模式配置为单数据组加密模式时, 只执行 128 比特数据加密, 此时设置加密密钥为 0x 66C6 C227 8E3B 8E05 3E7E A326 521B AD99, 明文输入为 0x 1387 F41E DD57 F3FB 9B9C 5B10 B514 CAD2, AES 加密模块双轮并行例化模块和双轮乒乓例化模块的实验结果密文输出均为 0x 60F9 EEDF 7F87 4C92 0AB1 7BFE 827D 9E66.

AES 的加密模式配置为双数据组加密模式时, 执行 2×128 比特数据加密, 此时设置加密密钥为 0x 66C6 C227 8E3B 8E05 3E7E A326 521B AD99, 明文输入分别为 0x 1387 F41E DD57 F3FB 9B9C 5B10 B514 CAD2 和 0x 0200 DEAF BABE BADC AB24 8000 0000 0001, AES 加密模块双轮并行例

化模块和双轮乒乓例化模块的实验结果相同, 仿真波形分别如图 8、图 9 所示, 两组明文对应的密文输出分别为 0x 60F9 EEDF 7F87 4C92 0AB1 7BFE 827D 9E66 和 0x AF65 6CCD 00CA B319 5E03 F945 F97B 969E.

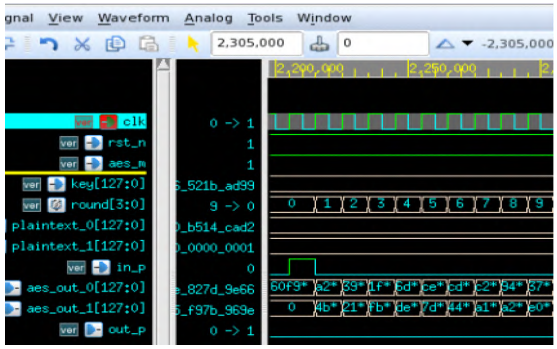

图 8　双数据组 AES 双轮并行加密实验结果

Figure 8　Results of AES double wheel parallel implementation

为了验证 RTL 代码功能正确性, 我们对 AES 算法进行了软件实现, 并将 RTL 仿真结果与软件加密模型对比, 经对比密文输出一致, 验证了 AES 两种例化方式的正确性. 为了对方案的功耗和面积进行评估, 我们在 TSMC 65 nm、tt_1p0v_25c 的工艺下用 Design Compiler 软件对不同方案的 AES-CCM 加密协议进行综合, 在 200 MHz 的时钟约束下, 传统双 AES 并行实现 AES-CCM 加密协议综合所得电路面积为 25.83 kgates, 功耗为 4.62 mW; 本方案所述 AES 双轮并行实现 AES-CCM 加密协议综合所得电路面积为 23.45 kgates, 功耗为 4.05 mW; 传统 AES 串行实现 AES-CCM 加密协议综合所得电路面积为 15.49 kgates, 功耗为 2.31 mW; 本方案所述 AES 双轮乒乓实现 AES-CCM 加密协议综合所得电路面积为 16.45 kgates, 功耗为 2.03 mW.

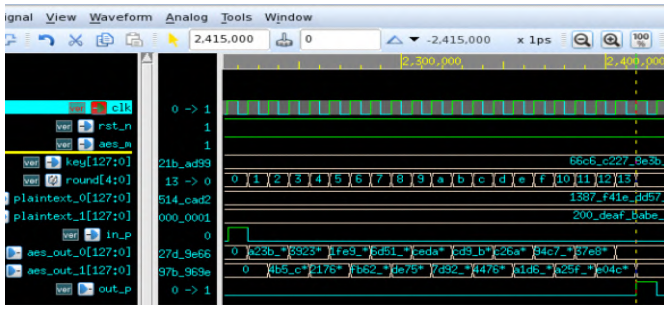

图 9　双数据组 AES 双轮乒乓加密实验结果

Figure 9　Results of AES double wheel ping-pang implementation

表 1　本方案与传统方案实现 AES-CCM 加密协议数据对比

Table 1　Comparison of AES-CCM encryption protocol data between proposed scheme and traditional scheme

方案	面积 kgates	功耗 uW/MHz
传统 AES 并行实现	25.83 (设为 100%)	4.62 (设为 100%)
本方案 AES 双轮并行实现	23.45 (设为 90.79%)	4.05 (设为 87.66%)
传统 AES 串行实现	15.49 (设为 100%)	2.31 (设为 100%)
本方案 AES 双轮乒乓实现	16.45 (设为 100.06%)	2.03 (设为 87.88%)

由以上分析可得与传统双 AES 并行实现 AES-CCM 方案相比, AES 双轮并行实现 AES-CCM 方案的面积和功耗分别减小 9.21% 和 12.34%; 与传统双 AES 串行实现 AES-CCM 方案相比, AES 双轮乒乓实现 AES-CCM 方案的面积增加 0.06%, 功耗减小 12.12%.

5 结论

本文根据 AES-CCM 链路层数据加密与解密都只用到 AES 加密模式, 且数据校验值生成与数据加解密密钥相同的特点, 给出基于 AES 双轮并行模块、AES 双轮乒乓模块的 AES-CCM 通用协处理器实现方案, 用户根据应用需求选择性例化实现. 方案中采用轮密钥共享机制, 以及 AES 算法 S 盒复合域化简实现方法, 有效去除冗余电路, 减小了电路功耗.

参考文献

[1] LAN/MAN Standards Committee. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications[S]. IEEE Std 802.11i-2004, IEEE Computer Society, 2004.

[2] NGUYEN K, LANANTE L, NAGAO Y, et al. Implementation of 2.6 Gbps super-high speed AES-CCM security protocol for IEEE 802.11i[C]. In: Proceedings of 13th International Symposium on Communications and Information Technologies: Communication and Information Technology for New Life Style Beyond the Cloud (ISCIT 2013). IEEE, 2013: 669–673. [DOI: 10.1109/ISCIT.2013.6645945]

[3] PAMMU A A, HO W G, LWIN N K Z, et al. A high throughput and secure authentication-encryption AES-CCM algorithm on asynchronous multicore processor[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(4): 1023–1036. [DOI: 10.1109/TIFS.2018.2869344]

[4] FENG B, QI D Y, HAN H W. General security co-processor implementation for MAC layer of wireless communication systems[J]. Microelectronics and Computer, 2013, 30(10): 33–37. [DOI: 10.19304/j.cnki.issn1000-7180.2013.10.009]
封斌, 齐德昱, 韩海雯. 无线通信系统 MAC 层通用安全协处理器的实现 [J]. 微电子学与计算机, 2013, 30(10): 33–37. [DOI: 10.19304/j.cnki.issn1000-7180.2013.10.009]

[5] CHEN Q Q. Design and Verification of AES Encrypt-and-Decrypt Module For Bluetooth 4.0[D]. Nanjing: Southeast University, 2015.
陈祺琦, 面向蓝牙 4.0 的 AES 加解密模块设计与验证 [D]. 南京: 东南大学, 2015.

[6] MORIOKA S, SATOH A. An optimized S-box circuit architecture for low power AES design[C]. In: Cryptographic Hardware and Embedded Systems—CHES 2002. Springer Berlin Heidelberg, 2002: 172–186. [DOI: 10.1007/3-540-36400-5_14]

[7] SATOH A, MORIOKA S, TAKANO K, et al. A compact Rijndael hardware architecture with S-box optimization[C]. In: Advances in Cryptology—ASIACRYPT 2001. Springer Berlin Heidelberg, 2001: 239–254. [DOI: 10.1007/3-540-45682-1_15]

[8] WOLKERSTORFER J, OSWALD E, LAMBERGER M. An ASIC implementation of the AES SBoxes[C]. In: Topics in Cryptology—CT-RSA 2002. Springer Berlin Heidelberg, 2002: 67–78. [DOI: 10.1007/3-540-45760-7_6]

作者信息

崔超 (1990–), 云南曲靖人, 硕士. 主要研究领域为集成电路设计和密码学.
cuichao2020@163.com

赵云 (1985–), 湖北荆门人, 博士. 主要研究领域为电力计量技术和信息安全技术.
zhaoyun@csg.cn

肖勇 (1978–), 湖南靖州人, 博士. 主要研究领域为电力计量技术和微电子技术.
xiaoyong@csg.cn

曾勇刚 (1963–), 四川威远人, 博士生. 主要研究领域为电力系统及自动化技术.
zengyg1@csg.cn

林伟斌 (1981–), 广东汕头人, 硕士. 主要研究领域为电力计量技术和密码学.
linweibin@csg.cn