·网络空间安全· 文章编号:1000-3428(2020)05-0167-07 文献标志码:A 中图分类号:TP391

一种面向密码 SoC 的高性能全双工 DMA 设计

吕广秋,李 伟,陈 韬,南龙梅

(信息工程大学 信息安全重点实验室,郑州 450001)

摘 要: 在密码 SoC 等数据密集型应用中,数据传输速度成为制约密码处理性能提升的瓶颈。结合密码 SoC 的数据流处理特点,提出一种面向密码 SoC 的高性能 DMA 优化设计方法。对特定模块的 DMA 传输开辟专用通道,利用并行读写数据提高特定模块 DMA 传输的总线带宽利用率。添加特殊工作模式用于自主控制重复任务传输以提升传输的带宽利用率。在此基础上,采用多通道优先级动态调整技术实现多任务下效率较高的自适应传输。仿真结果表明,该 DMA 在 55 nm 工艺下的最高频率达 910 MHz,总线利用率和协处理器利用率的平均值分别高达 91% 和 54% ,相对通用 DMA,其对密码 SoC 的 ZUC、SNOW、SM3、SM4 和 AES 算法的性能分别提升 216% 、222% 、123% 、69% 和 221% 。

关键词: 带宽利用率;读写并行;循环传输;动态优先级;自适应传输

开放科学(资源服务)标志码(OSID):

中文引用格式: 吕广秋,李伟,陈韬,等. 一种面向密码 SoC 的高性能全双工 DMA 设计[J]. 计算机工程,2020,46(5):167-173,180.

英文引用格式: LÜ Guangqiu,LI Wei,CHEN Tao,et al. A high performance full duplex DMA design for cryptographic SoC[J]. Computer Engineering,2020,46(5):167-173,180.

A High Performance Full Duplex DMA Design for Cryptographic SoC

LÜ Guangqiu,LI Wei,CHEN Tao,NAN Longmei

(Key Laboratory of Information Security,Information Engineering University,Zhengzhou 450001,China)

【Abstract】 In data-intensive applications such as cryptographic SoC,data transmission speed has gradually become a bottleneck restricting cipher processing performance. To address the problem,this paper proposes an optimized high performance DMA design method for cryptographic SoC based on the characteristics of stream processing in cryptographic SoC. First,a dedicated channel for DMA transfer of a specific module is opened,and data is read/written in parallel to improve the utilization rate of bus bandwidth in DMA transmission of a specific module. Second,a special work mode is added for autonomous control of repeated task transmission,so as to improve the utilization rate of transmission bandwidth. On this basis,dynamic adjustment technology based on multi-channel priority optimization is used to achieve more efficient adaptive transmission under multiple tasks. Simulation results show that the highest frequency of the proposed DMA in the 55 nm process is 910 MHz. The average utilization rate of bus and the coprocessor is 91% and 54% respectively. Compared with the general design of DMA,the proposed design increases the performance of ZUC,SNOW,SM3,SM4 and AES algorithms to cryptographic SoC by 216% ,222% ,123% ,69% and 221% respectively.

【Key words】 bandwidth utilization rate; read/write in parallel; cyclic transmission; dynamic priority; adaptive transmission

DOI: 10.19678/j.issn.1000-3428.0054776

0 概述

在密码片上系统(System of Chip,SoC)内集成专用协处理器以加速密码运算,已成为目前高性能 SoC 设计的重要方法。密码 SoC 的性能受主处理器、协处理器以及数据调度控制的影响[1-2],其中,直接内存存取(Direct Memory Access,DMA)设计尤为重要。DMA 的外围设备能直接访问内存,使其在内

基金项目: 国家自然科学基金(61404175)。

作者简介: 吕广秋(1994—),男,硕士研究生,主研方向为网络信息安全、集成电路设计;李 伟(通信作者),副教授、博士生导师;陈 韬、南龙梅,副教授。

收稿日期: 2019-04-29 **修回日期:** 2019-07-08 **E-mail:** 1205541637@qq.com

存数据拷贝[3-5]、实时数据采集[6-8]等数据密集型应用中得到广泛应用。

密码 SoC 等数据密集型应用对数据传输带宽的需求较高,因此,DMA 传输的总线带宽利用率直接影响密码 SoC 的整体性能。文献[9]中的 SoC 多层总线通信架构对 IP 在总线中的挂载分布提出更高要求,因此,其难以显著提高传输性能,且存在总线带宽利用率低、资源占用和功耗较大的缺点。文献[10-11]中更高性能的总线虽然具有更大带宽,但其在密码应用中总线带宽利用率以及重复任务和多任务传输效率均较低的问题仍未得到解决。

文献[12]提出一种支持链表和多通道传输的 DMA,其支持多个顺序固定的 DMA 传输,但具有密码协处理器利用率不高、重复任务和多任务传输效率低等不足。文献[13-15]提出基于双总线的全双工 DMA,虽然其实现了并行读写数据的功能,但总线闲置率过高且未提高同一总线上 IP 的 DMA 传输速度。文献[16]提出专用轻量级 DMA,其通过专用接口实现并行访问,但该 DMA 传输范围局限在固定 IP 与其他 IP 之间,难以支持任意 2 个 IP 之间的 DMA 传输。文献[17]使用多个 DMA 引擎实现数据预取,但其对无延迟的数据访问未取得优化效果。

本文借鉴已有研究根据特定应用优化 DMA 设计的思想[18-20],同时结合密码 SoC 数据流的特点,设计一种面向密码 SoC 的高性能全双工 DMA。针对总线带宽不足的问题,通过流水线技术对特定模块的 DMA 传输开辟专用通道以实现并行读写,无需更改总线结构,仅在特定模块接口和 DMA 读写控制器中进行少量更改便可大幅提高特定模块的 DMA 传输速度。针对 DMA 传输的控制、配置等时间过长的问题,本文 DMA 加入循环传输模式,实现 DMA 自主控制重复任务的循环执行,减少 CPU 启动、配置和返回等重复操作,提高传输效率和带宽利用率并降低 CPU 占用空间。针对协处理器利用率不高的问题,通过动态优先级技术完成各通道面向服务质量(Quality of Service,QoS)的自适应传输,进一步提高系统的传输效率和质量。

1 密码 SoC 性能分析

1.1 密码 SoC 内数据流特征分析

通用密码 SoC 包含通用主处理器 CPU、片上存储器、随机存储器 RAM、高速接口、DMA 和协处理器等部分,其结构如图 1 所示。通过分析密码服务特点可知,当密码 SoC 提供密码服务时,数据流向归总为 4 路 DMA 通道传输,如图 1 中虚线箭头所示:

①大量待处理数据由高速接口进入片内 RAM。

②片内 RAM 的数据进入协处理器并被处理。

③数据处理完成后返回 RAM。

④片内 RAM 中的数据传回高速接口完成一次密码服务。

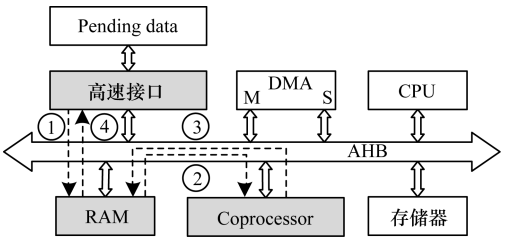

图 1 密码 SoC 中数据流特征

Fig. 1 Data stream characteristics in cryptographic SoC

1.2 密码 SoC 性能瓶颈分析

密码 SoC 的数据处理速度 V_P 主要由数据传输速度 V_T、协处理器利用率 α 和数据处理最大速度 V_{Co} 决定,即:

$$\max(V_P)=\min(V_T,\alpha\cdot V_{Co}) \tag{1}$$

协处理器的最大速度 V_{Co} 由本身硬件设计决定,本文不做讨论。数据传输速度 V_T 过低将会产生 2 种降低密码 SoC 性能的情况:

1)当协处理器数据传入速度 $V_{DataIn}<\alpha\cdot V_{Co}$ 时,将会出现数据断流,即协处理器必须等待数据输入。

2)当协处理器数据传出速度 $V_{DataOut}<\alpha\cdot V_{Co}$ 时,将会导致数据阻塞,即协处理器必须等待数据传出。

总线带宽利用率 β 定义如下:

$$\beta=\frac{t_D}{t_T}\times 100\% \tag{2}$$

其中,t_D 为数据传输周期数,t_T 为总线被 DMA 设备占用的时钟数。在理想情况下,传输 1 个数据最少花费 1 个时钟周期,即 β 最大为 100% 。

数据传输速度 V_T 等于整个密码服务期间 DMA 通道的数据平均传输速度 V_{DMA_ave}。当前密码 SoC 数据传输可用带宽 B 为:

$$B=\beta\cdot B_{max}=\sum_{i=1}^{n}V_{DMA\_i\_ave}+B_{其他} \tag{3}$$

其中,B_{max} 为系统总线的最大带宽,$V_{DMA\_i\_ave}$ 为 DMA 多个通道共用总线时第 i 个 DMA 通道的数据传输平均速度(本文中 $n=4$),$B_{其他}$ 为总线上其他操作占用的带宽。当 $B_{其他}=0$ 时,DMA 通道传输速度达到最大,由对称密码应用中各个 DMA 通道数据传输量相同得到:

$$V_{DMA\_i\_ave}\leqslant B_{max}\times\beta/n \tag{4}$$

DMA 传输是密码 SoC 最主要的数据传输方式,其直接决定带宽利用率 β 的大小。DMA 传输流程分为 4 步:

1)配置 DMA 传输。

2)DMA 将源地址数据读取至 FIFO。

3)DMA 将 FIFO 数据写入目的地址。

4)完成传输,挂起中断或等待 CPU 轮询。

由此可知,DMA 的传输速度为:

$$V_{DMA\_i}=\frac{L_B}{T_{Config}+T_{Start}+T_{DMA读}+T_{DMA写}+T_{DMA返回}} \tag{5}$$

其中,V_{DMA_i}为 DMA 启动传输到结束传输的平均速度,L_B为 DMA 传输的数据长度,T_{Config}为配置时间,T_{Start}和 $T_{DMA返回}$为传输启动和完成反馈的时间,$T_{DMA读}+T_{DMA写}$为 DMA 读写耗费时间。

在式(5)中,DMA 传输效率受定长时间的配置、启动和返回等操作影响,同时受由 DMA 读写方式决定的 DMA 读写耗费时间的影响。目前,学术界和工业界将 DMA 的读写方式分为三类,如表 1 所示。

表 1　3 种 DMA 读写方式的带宽利用率对比

Table 1　Comparison of bandwidth utilization rate of three read/write modes of DMA

DMA 读写方式	传输单个字最少花费的时钟数 m	带宽利用率 β/%	原理
数据逐个读取写入	3	<33	读取数据至少需要 2 拍,分为请求数据和返回数据 2 个阶段;写入数据因流水执行至少需要 1 拍
读取一组数据再写入	2	<50	读取数据和写入数据各至少需要 1 拍,流水执行数据读取和返回
并行读写(多总线实现)	1	<100	数据的请求、返回、写入全部实现流水执行

设 T_1为 $T_{Config}+T_{Start}+T_{DMA返回}$的值,不同 DMA 读写方式下的 DMA 传输速度为:

$$V_{DMA\_i}=\frac{L_B}{T_1+m\times L_B} \tag{6}$$

式(6)表明,传输数据长度 L_B越大,则 DMA 传输速率 V_{DMA_i}越高。本文中 L_B的单位为字(Word)且 T 的单位为时钟节拍数(Clock),此时有 $\beta=V_{DMA\_i}$。当 L_B足够大时有 $V_{DMA\_i}=\beta\approx 1/m$。

联合式(1)、式(4)和式(6)可知,密码 SoC 的数据处理速度 V_P可表示为:

$$\max(V_P)=\min\left(\frac{\beta\cdot B_{max}}{n},\alpha\cdot V_{Co}\right)=\min\left(\frac{L_B\cdot B_{max}}{(T_1+m\times L_B)\cdot n},\alpha\cdot V_{Co}\right) \tag{7}$$

由式(7)可知,密码 SoC 的最大数据处理速度 V_P无法大于总线可用带宽的 $1/n$ 或 $\alpha\cdot V_{Co}$。

密码 SoC 中的 B_{max}、V_{Co}和 L_B分别由总线类型、协处理器硬件设计和密码 SoC 数据处理分组长度决定,参数固定。为使得密码 SoC 性能最大化,本文将在影响因子 m、n、T_1、α 方面对 DMA 进行优化。

2　面向密码 SoC 的 DMA 分析

为提高密码 SoC 的性能,本文从 3 个方面对 DMA 设计进行优化:使用专用接口进行全双工的 DMA 读写传输,降低 DMA 重复配置与启动的时间,改变传输通道优先级的自适应传输。

由式(7)可知,密码 SoC 的性能由协处理器利用率决定,而协处理器利用率又受数据传输速度影响,因此,得到密码 SoC 性能最大化的必要条件和充分条件如下:

1)必要条件:数据传输速度 V_T足够大,不会限制协处理器利用率 α 和密码 SoC 性能。

2)充分条件:协处理器利用率 α 达到最大,此时密码 SoC 性能最大。

当密码 SoC 性能最大化的必要条件未满足时,设 V_P'为密码 SoC 的最大数据处理速度,由式(7)可知:

$$V_P'=\frac{L_B\cdot B_{max}}{(T_1+m\times L_B)\cdot n} \tag{8}$$

其中,影响因子 m、n 和 T_1对 V_P'的影响关系和取值范围如下:

$$\begin{cases} V_P'\propto\dfrac{1}{m},m\in\{1,2,3\} \\ V_P'\propto\dfrac{1}{n},n\in\mathbb{N}^+ \\ V_P'\propto\dfrac{1}{T_1},T_1\in\mathbb{N} \end{cases} \tag{9}$$

式(9)表明,为使得 SoC 性能最大化的必要条件未满足时 V_P'最大,应最小化 m、n 和 T_1。

本文在特定模块中开辟专用接口以实现并行读写的全双工 DMA 传输。由表 1 可知,此时 m 为最小值 1,且 AHB 总线上执行的 DMA 传输通道个数 n 由 4 降为 2。本文 DMA 专用接口占用硬件资源极小,在未改变系统总线结构的前提下实现了数据的全双工读写,极大地提高了数据传输速度并降低了总线传输负载。

本文 DMA 针对数据流向固定应用添加了自主传输的循环工作模式,使得 T_1最小化。每个通道各自具有独立的状态,且控制寄存器在传输完成后会重新置位,从而减少下一次配置、启动等的过程,即 DMA 与协处理器共同完成密码服务功能,无需 CPU 参与。除第一次 DMA 传输时需要进行配置,后续 DMA 通道传输的 $T_1=0$。当 DMA 工作在循环模式下完成多次 DMA 传输时,每次 DMA 通道传输的配置、启动等操作的平均值 $\bar{T}_1$ 趋于 0,将其代入式(6)得到总线带宽的平均利用率 $\bar{\beta}$ 为:

$$\bar{\beta}=\bar{V}_{DMA\_i}=\lim_{\bar{T}_1\to 0,m=1}\frac{L_B}{\bar{T}_1+m\times L_B}=1 \tag{10}$$

将 $\bar{T}_1$ 趋于 0 代入式(8),可知密码 SoC 的平均处理速度 $\overline{V'_P}$ 如式(11)所示:

$$\overline{V'_P}=\lim_{\bar{T}_1\to 0}\frac{L_B\cdot B_{max}}{n\times(\bar{T}_1+m\times L_B)}=\frac{B_{max}}{m\times n}\cdot\frac{Word}{Clock} \tag{11}$$

由式(10)、式(11)可知,本文 DMA 的循环工作模式使得总线带宽利用率和传输效率接近总线传输的理论上限值,从而最大化 DMA 的传输速度。当密码 SoC 性能最大化的必要条件满足后,密码 SoC 的性能受限于协处理器利用率 α,即:

$$V'_P=\alpha\cdot V_{Co} \tag{12}$$

为使协处理器利用率 α 最大,本文 DMA 采用多通道的动态优先级技术,实现了优先保证协处理器输入 FIFO 非空、输出 FIFO 非满,使得当 SoC 性能最大化的必要条件满足时协处理器利用率 α 接近 100% 且密码 SoC 的性能最大,最终实现密码 SoC 中数据的自适应传输。

将通用 DMA、链式 DMA 和本文 DMA 应用于密码 SoC 后,其协处理器利用率变化如图 2 所示。其中:

①为通用 DMA 等待 L_B 大小的数据处理完毕后再进行数据搬移时发生数据断流,协处理器处于空闲。

②为链式 DMA 提前传输 FIFO 中处理完毕的数据,数据断流得到缓解。

③为 DMA 传输优先保证协处理器输入 FIFO 非空、输出 FIFO 非满,消除数据断流和阻塞,最大化协处理器利用率 α,从而极大地提高了密码 SoC 性能。

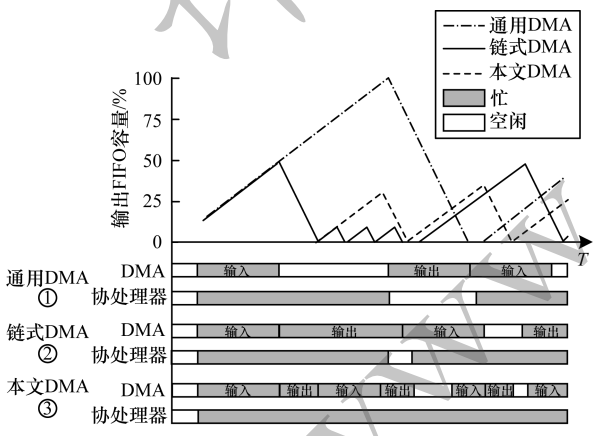

图 2 3 种 DMA 传输方式下的协处理器利用率变化

Fig. 2 Varying utilization rate of coprocessor in three transmission modes of DMA

3 面向密码 SoC 的 DMA 设计

3.1 DMA 硬件结构

相较于传统 DMA,本文 DMA 具有支持全双工数据读写、循环工作模式和自适应传输功能,其硬件结构如图 3 所示。其中,①完成全双式数据读写,②中的读写状态机采用循环工作模式,③具备自适应传输功能,④为 DMA 各通道的配置参数。

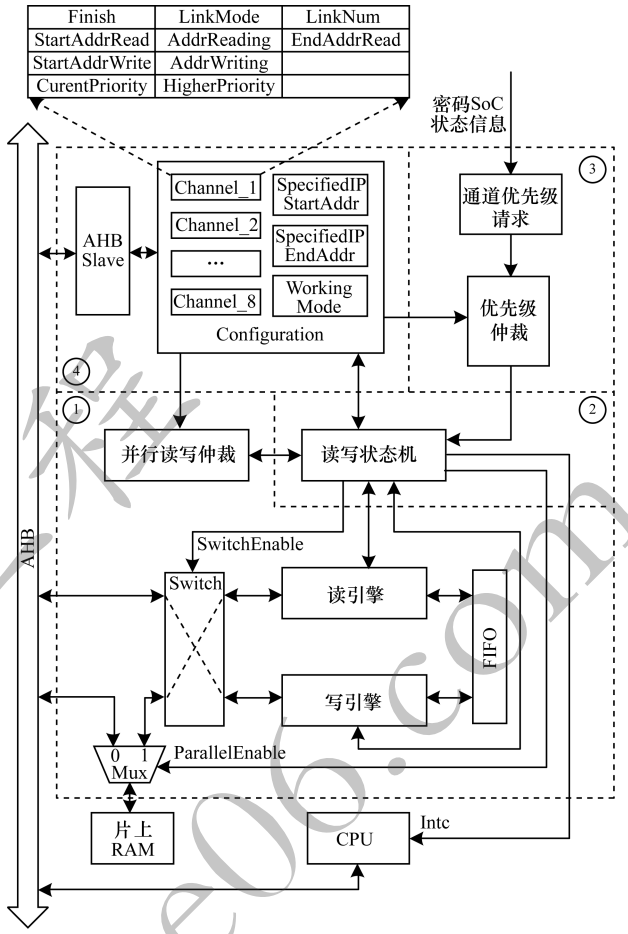

图 3 DMA 硬件结构

Fig. 3 DMA hardware structure

在图 3 中,由并行读写仲裁电路决定是否进行全双工读写,其控制电路如图 4 所示。

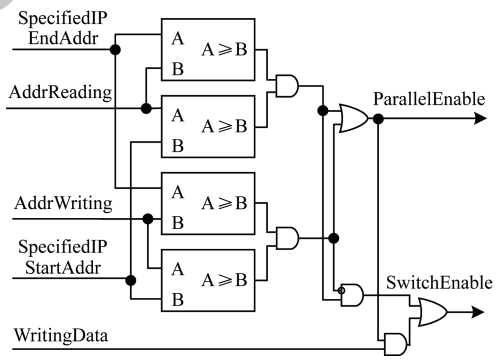

图 4 并行读写仲裁控制电路

Fig. 4 Parallel read/write arbitration control circuit

当 ParallelEnable 为高电平有效时,本文 DMA 处于全双工并行读写状态,此时由 ParallelEnable 和 SwitchEnable 信号共同决定读写引擎对片上 IP 和 RAM 的控制通路。本文 DMA 的循环工作模式由图 3中的部分②完成。一旦通道传输完毕,读写状态机检测到该通道工作在循环模式时,会将该通道的配置寄存器 AddrReading 和 AddrWriting 重新赋值为

StartAddrRead 和 StartAddrWrite,并且不会对通道完成标志信号 Finish 置位,即该通道重新配置为传输初始状态,减轻 CPU 对重复任务的控制负担。

自适应传输由图 3 中的部分③完成。由通道优先级请求电路和优先级仲裁电路共同完成通道优先级的动态调整,最终实现协处理器输入 FIFO 非空、输出 FIFO 非满。为实现该目标,本文 DMA 使用通道优先级请求电路生成通道的提权请求信号 Priority_Higher。同时,为了保证循环模式下的数据一致性,该模块生成了通道的挂起请求信号 Priority_Suspend,例如,当发生数据覆盖或读取未准备好的数据时,当前通道传输应当挂起。通道优先级请求信号生成关系如表 2 所示。优先级仲裁电路会根据通道的挂起、提权信号选定每个通道当前优先级,通过仲裁实时得到优先级最高的通道,并通知读写状态机将总线授权给该通道以进行读写。

表 2　各通道的动态优先级

Table 2　Dynamic priority of each channel

通道编号	初始优先级	挂起优先级	提权优先级	通道挂起条件(Priority_Suspend)	通道提权条件(Priority_Higher)
1	4	0	1	接口输入 FIFO 空或 RAM 输入空间满	通道未挂起且 RAM 输入空间几乎空
2	2	0	1	RAM 输入空间空或协处理器输入 FIFO 满	通道未挂起且协处理器输入 FIFO 几乎空
3	2	0	1	RAM 输出空间满或协处理器输出 FIFO 空	通道未挂起且协处理器输出 FIFO 几乎满
4	4	0	1	接口输出 FIFO 满或 RAM 输出空间空	通道未挂起且 RAM 输出空间几乎满

3.2　DMA 工作流程

本文 DMA 工作流程如图 5 所示。

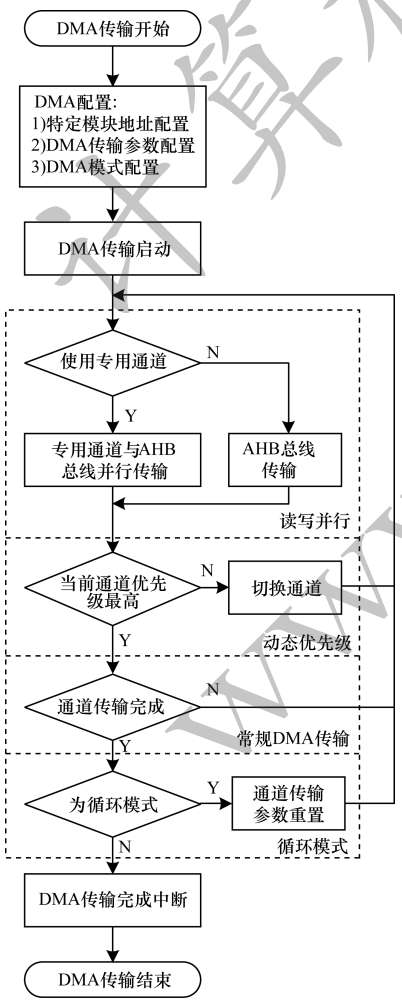

图 5　DMA 工作流程

Fig. 5　DMA workflow

在 DMA 传输配置阶段需要对使用专用接口的特定模块地址范围、各个通道的传输参数以及工作模式进行配置。在 DMA 传输开始后,首先检测当前传输通道的源或目的地址是否包含在专用接口的地址范围内,如果是,则使用 AHB 总线和专用通道并行读写数据,高效实现数据搬移,此时 $m = 1$;否则,DMA 将定长大小的数据块读入 FIFO 后写至目的地址,流水执行数据的读取和返回,此时 $m = 2$。优先级仲裁器接收到通道传输状态反馈后进行通道优先级动态调整,实现面向 QoS 的自适应传输:当通道提权信号有效时,通道提升到预配置的高优先级;当挂起信号有效时,当前通道传输挂起,由次优先级通道进行传输或进入等待状态;通道的提权和挂起信号均无效时则优先级不变。

图 6 所示为面向 QoS 的自适应传输示例。自适应传输允许优先级较高的通道挂起优先级较低的通道传输(如 Task1 ~ Task3),而传统 DMA 不允许通道传输被打断,导致当前传输通道优先级可能不是最高。同时,本文 DMA 自适应传输优先在当前最高优先级通道中准备完毕的通道中进行传输(如 Task3 挂起,执行 Task4),并且自适应传输允许通道优先级动态变化(如 Task5),从而提高传输服务质量。当工作在循环模式时,DMA 通道在完成传输后自动重置传输参数,节省 CPU 对 DMA 配置、启动等的时间,高效执行重复的 DMA 传输任务。在不启用循环模式时,DMA 完成一次传输后,通常由中断模块向 CPU 发起中断报告传输完成情况。

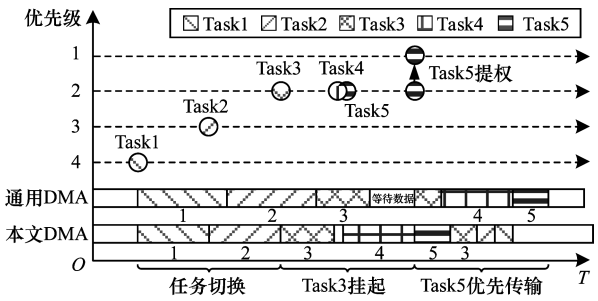

图 6 面向 QoS 的自适应传输示例

Fig. 6 Example of adaptive transmission for QoS

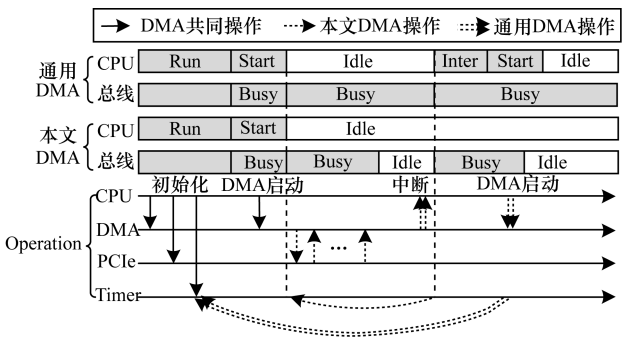

图 7 循环模式传输效率优化效果

Fig. 7 Effect of transmission efficiency optimization in the cyclic mode

图 7 所示为 DMA 在 2 种模式下的传输效率对比,单实线为通用 DMA 与本文 DMA 共同操作,双虚线为通用 DMA 完成一次通道传输后返回和重新配置操作。从图 7 可以看出,DMA 工作在循环模式时无需 CPU 参与,提高了总线带宽利用率 β 和 SoC 应用的灵活性。

4 实验评估

为对本文 DMA 进行有效评估,将其与文献[12-14]中的 DMA 以及由 Design Ware2018 生成的 DMA 进行对比分析,结果如表 3 所示。

表 3 DMA 的性能对比分析

Table 3 Comparison and analysis of DMA performance

DMA	硬件设计					通道仲裁策略				工作模式				*m*	
	资源消耗/KGate	最高频率/MHz	总线类型	传输位宽	通道个数	固定优先级	轮转优先级	令牌优先级	动态优先级	普通模式	链表模式	循环模式	读写并行	特定模块	普通模块
本文 DMA	28	910	AHB	32	8	✓			✓	✓	✓		✓	1	2
Design Ware2018 生成的 DMA	23	956	AHB	32	8	✓	✓	✓		✓	✓			3	3
文献[12]DMA	34	731	AHB	8/16/32/64	16	✓				✓	✓			2	2
文献[13]DMA	—	—	AHB	32	8	✓				✓	✓		✓	1	2
文献[14]DMA	—	—	AHB	64	64	✓				✓			✓	1	2

在表 3 中,本文 DMA 采用 Verilog HDL 硬件语言实现,并基于 55 nm 工艺对设计进行逻辑综合。最高频率是指将 DMA 设计的频率从原工艺等效至 55 nm下所得到的大致工作频率,✓表示支持该功能,—表示文中未给出。由表 3 可知,本文 DMA 消耗资源适中,频率较高,在通道个数、传输位宽上相对文献[12]与文献[14]DMA 较少。虽然本文 DMA 相对 Design Ware2018 生成的 DMA 仲裁策略不足,但其在工作模式和读写并行上功能完善,对密码应用的支持性更好。

当对外提供密码服务且时钟频率为 400 MHz 时,传输分片长度 L_B 对通用 DMA 与本文 DMA 的数据传输速度及总线带宽利用率 β 的影响如图 8 所示。其中,通用 DMA 带宽利用率变化曲线与式(6)吻合,而本文 DMA 因后续通道传输没有配置、启动等时间,导致传输效率几乎不随 L_B 变化。本文 DMA 使用专用接口进行并发读写源、目的地址,V_{DMA_i} 可达 11.6 Gb/s,而通用 DMA 只能进行数据的逐个读取写入,V_{DMA_i} 仅为 3.4 Gb/s。

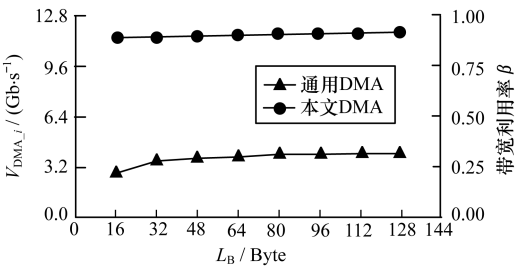

图 8 400 MHz 下 DMA 传输效率随 L_B 的变化情况

Fig. 8 DMA transmission efficiency changing with L_B at 400 MHz

表 4 所示为本文 DMA 对对称密码服务的性能优化情况。从表 4 可以看出,相对通用 DMA,应用本文 DMA 后带宽利用率平均值由 28% 上升至 91%,协处理器利用率平均值由 25% 上升至 54%,密码算法 ZUC、SNOW、SM3、SM4 和 AES 的性能分别提升了 216%、222%、123%、69% 和 221%。

表 4　DMA 传输下对称密码算法实验结果

Table 4　Experimental results of symmetric cipher algorithm in DMA transmission

算法	运算轮数	理论吞吐率/(Mb·s^{-1})	DMA	吞吐率/(Mb·s^{-1})	协处理器利用率 α/%	带宽利用率 β/%	性能提升/%
ZUC	1	12 800	本文	2 912	23	91	216
			通用	921	7	28	
SNOW	1	12 800	本文	2 943	23	92	222
			通用	913	7	27	
SM3	65	3 938	本文	3 890	98	87	123
			通用	1 745	44	27	
SM4	32	1 600	本文	1 584	97	93	69
			通用	937	59	29	
AES	10	10 662	本文	3 007	28	94	221
			通用	936	9	29	

5　结束语

本文对密码 SoC 中基于 AHB 总线的 DMA 传输进行优化,为特定模块开辟专用接口实现并行读写,使用循环模式和动态优先级技术完成 DMA 通道的高效传输,从而解决通用 DMA 使用 AHB 总线时带宽利用率低的问题,提高密码 SoC 的整体性能。实验结果表明,相对通用 DMA,本文 DMA 的协处理器利用率与带宽利用率均较高。然而本文 DMA 还存在不支持描述符配置和仅支持 AHB 总线接口等不足,探究并解决该问题将是下一步的研究方向。

参考文献

[1] SHANEHSAZZADEH F, SADRI M S. Area and performance evaluation of central DMA controller in Xilinx embedded FPGA designs[C]//Proceedings of 2017 Iranian Conference on Electrical Engineering. Washington D. C., USA:IEEE Press,2017:25-63.

[2] ROTA L,CASELLE M,CHILINGARYAN S,et al. A new DMA PCIe architecture for Gigabyte data transmission[C]//Proceedings of the 19th IEEE-NPSS Real Time Conference. Washington D. C.,USA:IEEE Press,2014:46-65.

[3] SU Yonghai, HUANG Li. FPGA design of multi-channel dynamic-priority DMA system based on PCI Express[J]. Communications Technology, 2017, 50(7): 1570-1575. (in Chinese)
苏永海,黄莉. 基于 PCI Express 的多通道动态优先级 DMA 系统的 FPGA 设计[J]. 通信技术,2017,50(7):1570-1575.

[4] VUJIC N,CABARCAS F,GONZALEZ TALLADA M,et al. DMA + +:on the fly data realignment for on-chip memories[J]. IEEE Transactions on Computers,2012,61(2):237-250.

[5] LI Shenglan,JIANG Hongxu,FU Weijian,et al. Design of DMA controller for multi-channel transmission system based on PCIe[J]. Journal of Computer Applications,2017,37(3):691-694,716. (in Chinese)
李胜蓝,姜宏旭,符炜剑,等. 基于 PCIe 的多路传输系统的 DMA 控制器设计[J]. 计算机应用,2017,37(3):691-694,716.

[6] ENAMI T,KAWAKAMI K,YAMAZAKI H. DMA-driven control method for low power sensor node [C]//Proceedings of 2015 IEEE Topical Conference on Wireless Sensors and Sensor Networks. Washington D. C., USA: IEEE Press,2015:52-85.

[7] KACEM H, GLAOUI M, GHARSALLAH A. Power saving solution for WSN cases studies based on interrupt handler versus DMA[C]//Proceedings of International Multi-Conference on Systems. Washington D. C., USA: IEEE Press,2015:256-278.

[8] ROTA L,CASELLE M,CHILINGARYAN S,et al. A PCIe DMA architecture for multi-gigabyte per second data transmission[J]. IEEE Transactions on Nuclear Science,2015,62(3):972-976.

[9] MEDARDONI S, RUGGIERO M, BERTOZZI D, et al. Interactive presentation: capturing the interaction of the communication, memory and I/O subsystems in memory-centric industrial MPSoC platforms[C]//Proceedings of 2007 Design, Automation & Test in Europe Conference & Exhibition. Washington D. C., USA: IEEE Press, 2007: 1245-1256.

[10] ARM Ltd. AMBA 5.0 specifications[EB/OL]. [2019-03-25]. https://developer.arm.com/products/architecture/system-architectures/amba/amba-5.

[11] NARMADHA N, MITHYA V. Performance analysis of ADMA on bus based SoC-survey[C]//Proceedings of 2015 Online International Conference on Green Engineering and Technologies (IC-GET). Washington D. C., USA: IEEE Press,2015:23-56.

[12] LI Bing,PAN Shengmin,DU Qing,et al. Enhanced DMA controller based on AMBA bus:CN201510167612.4[P]. 2015-07-01. (in Chinese)
李冰,潘胜民,杜清,等. 基于 AMBA 总线的增强型 DMA 控制器:CN201510167612.4[P]. 2015-07-01.

[13] SHI Wenxia, WU Longsheng, SHENG Tingyi, et al. Design of DMA controller supporting full-duplex data transmission and multi-channel[J]. Microelectronics and Computer,2015,32(2):76-79,83. (in Chinese)
石文侠,吴龙胜,盛廷义,等. 一种支持全双工数据传输的多通道 DMA 控制器设计[J]. 微电子学与计算机,2015,32(2):76-79,83.

[14] YU Zaixiang,CHEN Haibo,SUN Yongjie,et al. Design and implementation of the parallel transmission mechanism in the direct memory access controller[J]. Microelectronics and Computer,2012,29(2):1-6. (in Chinese)

(下转第 180 页)

(上接第 173 页)

余再祥,陈海波,孙永节,等. DMA 并行传输机制的设计与实现[J]. 微电子学与计算机,2012,29(2):1-6.

[15] ZHANG Luyu, LI Li, PAN Hongbing, et al. Design of a multi-interface DMA controller based on SoC [J]. Electronic Measurement Technology, 2014, 37(9): 32-36. (in Chinese)
张路煜,李丽,潘红兵,等. SoC 系统中多端口 DMA 控制器的设计[J]. 电子测量技术,2014,37(9):32-36.

[16] OLUGBON A, KHAWAM S, ARSLAN T, et al. An AMBA AHB-based reconfigurable SoC architecture using multiplicity of dedicated fly by DMA blocks[C]//Proceedings of Design Automation Conference. Washington D. C., USA: IEEE Press, 2005: 259-278.

[17] HUANG Kan, TONG Dong, LIU Yang, et al. MCS-DMA: an optimized design of memory controller for DMA transmission in SoC[J]. Acta Electronica Sinica, 2010, 38(3): 598-604. (in Chinese)
黄侃,佟冬,刘洋,等. MCS-DMA:一种面向 SoC 内 DMA 传输的内存控制器优化设计[J]. 电子学报,2010,38(3):598-604.

[18] CHEN K, QI L, YU H. Design of two-dimension DMA controller in media multi-processor SoC [C]// Proceedings of Workshop on Intelligent Information Technology Applications. Washington D. C., USA: IEEE Press, 2008: 52-63.

[19] YU C H, LIU C K, KANG C H, et al. An efficient DMA controller for multimedia application in MPU based SoC[C]//Proceedings of IEEE International Conference on Multimedia and Expo. Washington D. C., USA: IEEE Press, 2007: 988-1023.

[20] KURTH A, VOGEL P, MARONGIU A, et al. Scalable and efficient virtual memory sharing in heterogeneous SoCs with TLB prefetching and MMU-Aware DMA engine[C]// Proceedings of 2018 IEEE International Conference on Computer Design. Washington D. C., USA: IEEE Press, 2018: 566-589.

编辑　吴云芳