基于Amdahl定律的异构多核密码处理器能效模型研究

李 伟,郎俊豪*,陈 韬,南龙梅
(战略支援部队信息工程大学,河南郑州 450000)

摘 要: 边缘计算安全的资源受限特征及各种新型密码技术的应用,对多核密码处理器的高能效、异构性提出需求,但当前尚缺乏相关的异构多核能效模型研究. 本文基于扩展Amdahl定律,引入密码串并特征、异构多核结构、数据准备时间、动态电压频率调节等因素,将核划分空闲、活跃状态,建立异构多核密码处理器的能效模型. MATLAB仿真结果表明,数据准备时间占比小于10%时,对能效的负面影响大幅下降;固定电压,频率缩放会影响能效值大小;处理器核空闲/活跃能耗比例越小,能效值越大. 架构上,固定异构核,同构核数量与密码任务最大并行度相等时能效值最大,最佳异构核数可由模型变化参数仿真得到;多任务调度执行上,流水与并发执行有利于能效值的进一步提升. 多核密码处理器芯片板级测试结果表明,仿真结果与实测数据相关系数接近1,芯片实测的数据准备时间、电压频率缩放等因素的影响与仿真分析基本一致,验证了所提能效模型的有效性. 该文重点从影响能效变化趋势因素上,为多核密码处理器异构、高能效设计提供一定的理论分析基础与建议.

关键词: 密码处理器;多核处理器;异构;Amdahl定律;能效模型
基金项目: 国家自然科学基金(No.61404175);河南省科技攻关项目(No.202102210116)
中图分类号: TN492;TP309.7 **文献标识码:** A **文章编号:** 0372-2112(2024)03-0849-14
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220839

Amdahl's Law-Based Energy-Efficient Model for Heterogeneous Multicore Crypto-Processor

LI Wei, LANG Jun-hao*, CHEN Tao, NAN Long-mei
(*PLA Information Engineering University*, *Zhengzhou*, *Henan* 450000, *China*)

Abstract: The resource constraints of Edge Computing security and application of new cryptography technologies require the high energy efficiency and heterogeneity of multi-core cryptoprocessors, but there is still a lack of energy-efficient model. Based on extending Amdahl's law, this paper introduces the feature of cipher, heterogeneous multicore structure, data preparation time, dynamic voltage and frequency scaling, divides cores into idle and active states, then builds the energy-efficient model of heterogeneous multicore cryptoprocessor. MATLAB simulations show that the negative impact on energy efficiency is considerably reduced when the data preparation time is less than 10%. Fixed voltage and frequency scaling can affect the value of energy efficiency. The smaller the idle/active energy ratio of the processor core, the larger the energy efficiency value. On the architecture side, when the number of homogeneous cores is equal to the maximum parallelism of the cryptograph task, the energy efficiency value is largest when the number of heterogeneous cores is fixed, and the optimal number of heterogeneous cores can be simulated by varying the parameters of the model. In the execution of multi-task scheduling, pipelines and concurrent execution are beneficial to further increase the energy efficiency value. Board-level test results show that the correlation coefficient between simulation results and chip test data is close to 1, and the influence of measured data preparation time, voltage frequency scaling and other factors is essentially consistent with the simulation analysis, which verifies the effectiveness of the proposed energy efficiency model. In this paper, we focus on the factors affecting the energy efficiency trend and provide some theoretical analytical grounds and recommendations for heterogeneous and energy efficient design of multicore cryptographic processors.

收稿日期:2022-07-18;修回日期:2023-01-31;责任编辑:孙瑶
*通讯作者:郎俊豪

Key words: crypto-processor; multicore processor; heterogeneous; Amdahl's law; energy-efficient model
Foundation Item(s): National Natural Science Foundation of China (No.61404175); Scientific and Technological Project of Henan Province (No.202102210116)

1 引言

在物联网、大数据、人工智能等新一代信息技术与制造技术深度融合背景下,工业互联网迅速发展. 安全作为工业互联网三大功能体系之一,是网络与数据在工业中应用的重要保障[1]. 密码处理器作为密码算法的实现载体,提供各类密码服务保障数据的安全与隐私,满足不同安全场景需求. 边缘计算安全是工业互联网安全的重要环节,不同于节点设备的轻量级要求和中心计算的高性能要求,边缘设备的实时性、资源受限等特征[2],要求其同时兼顾性能与能耗,这对密码处理器的性能与能耗权衡提出了挑战.

能效值是衡量性能与能耗平衡的重要指标,一般表述为单位能耗所获得的性能(以 Mbps/mW 或 Bit/J 为单位). 密码算法操作密集、数据量大的特点易导致大量能量消耗,因此传统单核密码处理器尽管采用架构优化、存内/近存计算、定制单元等优化方式[3~5],但能效值提升碰到了瓶颈. 同构多核密码处理器采用同构结构,在性能上提升较大,但同时也造成功耗的增大. 在通用计算领域,采用异构方式的多核处理器在能效上获得了较大提升[6]. 同时,随着抗量子密码算法、同态签名等新密码技术出现[7,8],对多核密码处理器灵活性提出挑战;另外,在现实需求场景中,如 IPsec 协议、DTLS 协议等往往需要同时支持公钥密码、对称密码、杂凑函数等,异构核方式更适用于同时实现不同密码体制以提升多核密码处理器能效. 然而当前对多核密码处理器能效模型的研究较少,理论基础缺乏. 该文基于 Amdahl 定律对异构多核密码处理器能效模型进行研究,综合考虑密码算法串并特征、数据准备时间、动态电压频率调节(Dynamical Voltage and Frequency Scaling,DVFS)技术等影响,构建异构多核密码处理器的性能模型与功耗模型,进而得到能效模型,并进一步分析处理多密码任务调度方式对能效值的影响,为高能效多核密码处理器的设计提供一定的理论支撑与建议.

2 Amdahl 定律研究

Amdahl 定律最早由 IBM 的 Amdahl 博士进行描述[9],即系统采用并行化技术后,所能获得的性能极限取决于并行化部分所占比例. Amdahl 定律可抽象表示为式(1),其中,$S(f,n)$表示系统获得的加速比,f表示系统串行部分所占比例,$1-f$为并行部分所占比例,n表示系统并行部分并行度. Amdahl 的本质是在固定处理任务规模前提下,通过比较并行优化前后系统处理任务的时间得到系统加速比.

$$S(f,n)=\frac{1}{f+\frac{1-f}{n}} \tag{1}$$

国内外学者基于 Amdahl 定律对处理器性能与能耗扩展建模做了许多研究. 文献[10]将处理器核抽象成基本等价核(Base Core Equivalents,BCE),基于 BCE 概念对同构、异构、动态这 3 种多核处理器架构进行性能建模,但其性能模型较为简单,未考虑数据通信等因素影响. 文献[11]扩展 Amdahl 定律建立了多核处理器的性能、功耗模型,在功耗模型中提出将处理器核分成活跃、空闲这 2 个状态建模,但模型考虑实际影响因素较少,且受限于 Amdahl 定律的基本假设,模型准确度不高. 文献[12]构建了集成 CPU 和 GPU 处理器核的异构多核处理器性能、功耗模型,结果表明异构多核处理器在能效值上表现更好. 文献[13]针对多核密码处理器性能建模,考虑密码任务特征、数据传输时间、同步时间对性能的影响,但文献以探索高性能设计空间为目标,并未考虑能效建模. 文献[14]考虑多核处理器中数据准备时间(非计算时间)对性能模型的影响,扩展 Amdahl 定律,引入数据准备时间对多核性能模型进行修正. 文献[15]对使用 Intel 的 Turbo-Boost 技术的多核处理器扩展 Amdahl 定律建模,说明动态频率变化对多核处理器性能的增益. 文献[16]基于当前多核处理器存在多种类型异构核的现实,扩展 Amdahl 定律,建立多种类型异构核处理器架构的性能与功耗模型,结果表明多种类型异构核多核处理器更匹配各类任务特征,在性能与功耗的权衡上能取得更好的结果.

本文在现有扩展 Amdahl 定律研究基础上,以研究异构多核密码处理器能效影响因素和探索高能效设计空间为目的,构建异构多核密码处理器能效模型. 模型重点考虑:引入数据准备时间消耗、DVFS 技术增益正反两方面的影响;对不同密码任务特点,研究多种类型异构核的多核密码处理器架构能效变化趋势;在密码任务段划分上,结合实际密码特征,弥补 Amdahl 定律完全串行、无限并行假设的不足;同时考虑多密码任务调度执行方式对能效值的影响.

3 异构多核密码处理器能效模型

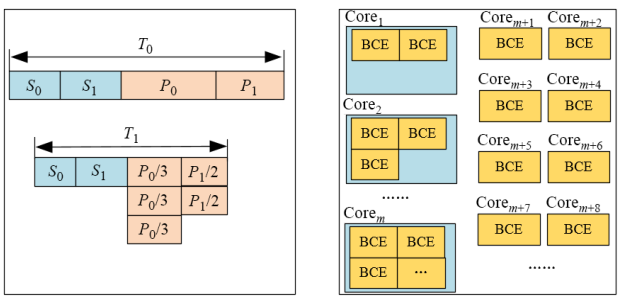
3.1 异构多核密码处理器架构分析

现有研究表明,异构多核处理器架构在能效上有更好的表现[12]. 异构多核密码处理器提升密码任务执行能效主要表现在两方面:一是通过开发密码任务并行性,提升性能的同时,不造成等比例能耗开销;二是

通过异构结构,与密码任务的执行特征相适应,提升任务串行部分性能的同时,减少执行的能耗. 并行性、密码任务适应性是异构多核密码处理器能够提升能效的两个关键点.

Amdahl定律假设任务能被分成串行、无限并行两部分,但对密码任务,这个假设过于简化. 由于操作数据量密集、运算频繁等特点,密码任务的划分不只是简单的串行、并行. 具体来说,密码任务的串行执行部分可能不只有一种粒度的操作,其并行执行部分也不是完全并行,而是分段式的部分并行. 现有的异构多核密码处理器研究只针对"单异构核加同构核"的方式[13]. 为进一步探索异构多核密码处理器能效提升潜力,本文对多个不同类型异构核加同构核的多核密码处理器架构进行研究.

为简化多种类型异构核的多核密码处理器的描述与建模,借鉴等价基本核BCE的思想[10],假设不同类型的异构核由不同数量的BCE组成,1个BCE代表1个同构核. 异构多核密码处理器架构总体由N个BCE组成,其中有m个不同类型的异构核. 如图1所示,图1(a)表示单个BCE上执行密码算法时间为T_0,在异构多核密码处理器上,由于串行段特征不同,可以将其划分为S_0和S_1,并行任务部分可以划分成两个并行度分别为3和2的并行段. 图1(b)表示异构多核处理器架构由m个不同类型的异构核和由多个单BCE表示的同构核组成. 根据密码划分特征,可以将图1(a)的串行部分S_0和S_1映射到不同的异构核,适应密码任务特点,并行部分可以映射到同构核上提升并行度.



(a) 密码任务划分举例　　(b) 异构多核密码处理器架构

图1　密码任务划分与异构多核处理器示意图

模型中涉及的变量如表1所示,所有变量可划分成异构多核配置、密码任务串并行变量、性能变量、功耗变量、DVFS技术影响性能、DVFS技术影响功耗共6类. 其中异构多核配置、密码任务串并行变量的选取,一是源自实际异构多核密码处理器及密码任务串行、并行部分的特征分析与提取,二是参考现有模型相关的研究[10,16];性能变量、功耗变量的选取主要考虑便于建立性能、能耗模型,进而得到能效模型,一是结合实际影响异构多核密码处理器运行性能、功耗的参数,二是分析现有基于Amdahl定律的性能、功耗模型研究得到[11~13];DVFS技术影响性能、功耗模型参数,主要基于DVFS技术对能效值有着重要影响的考量,引入相关参数以提高模型与实际现有技术的结合度,其参数选取一方面经分析异构多核密码处理器功耗来源得到,另一方面结合了DVFS技术相关的研究[15]. 实际上,对表1中模型参数的选取和准确性研究,除基于异构多核、密码任务、性能、功耗等方面的实际情况分析,参考之前相关的模型研究工作外,还在后续多核密码处理器芯片板级实测中对各类参数构建起的整个能效模型进行验证.

3.2　性能模型建立

异构多核密码处理器的性能模型主要基于Amdahl定律,为便于后续能效值对比分析,假设单个BCE同构核上完成密码任务需要时间为1,性能为1. 为让性能模型更加符合实际情况,考虑从数据准备时间消耗、DVFS技术增益正反两个方面修正模型. 由N个BCE组成的异构多核密码处理器完成密码任务时间可用式(2)表示:

$$T_{\mathrm{N}}=f_{\mathrm{DVFS}}\cdot\left(T_{\mathrm{s}}+T_{\mathrm{p}}\right)\cdot\left(1-g(N)\right)+g(N) \tag{2}$$

其中,$g(N)$($0<g(N)<1$)表示数据准备时间占总时间的比例,是关于N的函数;f_{DVFS}是DVFS技术给异构多核密码处理器性能带来的影响参数;T_{s}表示串行执行时间;T_{p}表示并行执行时间. 下面将分别对各个参数进行分析.

(1)串行执行时间T_{s}. 密码任务实际映射到多核时,由于密码算法结构特征,划分的串行密码任务段又可以再被划分成几个不同粒度的串行段(如协议中同时使用非对称密码算法和对称密码算法时),这些串行段在不同的异构核上执行能够更适应任务特征,得到更好的能效结果. 假设m个异构核,性能用向量$\boldsymbol{S}=(s_1,s_2,\cdots,s_m)$($0<s_i<1, 1\leqslant i\leqslant m$)表示,$s_i$表示第$i$个异构核相比于单个BCE同构核的性能缩放比,$s_i<1$表示异构核执行串行任务比同构核消耗更少时间. 向量$\boldsymbol{Q}=(q_1,q_2,\cdots,q_m)$($0<q_i<1$)表示密码任务串行部分中的$m$个串行任务分段. 向量$\boldsymbol{R}=(r_1,r_2,\cdots,r_m)$表示$m$个异构核是否被使用,$r_i$($1\leqslant i\leqslant m$)只取0或1. 当$q_i=0$时,表示第$i$个异构核无串行段任务执行,此时$r_i$也为0. 串行执行时间$T_{\mathrm{s}}$可表示为式(3):

$$T_{\mathrm{s}}=\sum_{i=1}^{m}\left(r_i\cdot s_i\cdot q_i\right),\ r_i\in\{0,1\} \tag{3}$$

除m个异构核外,为表示余下同构核的数量,根据波拉克法则[17],处理器性能与面积相关,而面积又可以用等价BCE核来表示,进而得到异构核性能$\boldsymbol{S}$与等价BCE核关系,假设用σ/s_i表示第i个异构核的等价BCE

表1 模型参数说明表

类型	参数名	说明
异构多核配置	N	多核处理器BCE总核数
	m	异构处理器核数
	N_{homo}	同构处理器核数
性能变量	T_{N}	密码任务总完成时间
	T_{p}, T_{s}	并行、串行部分密码任务计算时间
	$g(N)$	数据调度准备消耗时间
密码任务串、并行变量	$\boldsymbol{R}$	是否使用异构核向量
	$\boldsymbol{S}$	异构核性能向量
	$\boldsymbol{Q}$	任务串行部分各分段占比
	P, f_j	并行部分分段值、各分段占比($1\leqslant j\leqslant P$)
	p_j	各并行分段的并行度
DVFS影响性能	Fre, ρ	工作频率、频率对性能影响的比例参数
	σ	异构核BCE比例参数
功耗变量	E_{N}	密码任务完成总能耗
	E_{s}, E_{p}, E_{DP}	串行计算、并行计算、数据调度准备能耗
	E, K	异构核活跃能耗、异构核空闲能耗
	K_{s}, e_{dp}	同构核空闲能耗比例、数据准备平均能耗
DVFS影响功耗	Dyn, Sta	DVFS技术对动态、静态功耗影响
	V, γ, λ	工作电压、频率影响功耗比例参数、电压影响功耗比例参数

个数，其中σ为比例系数(实际上，不同类型异构核的σ应该不同，为简化模型，统一用σ表示)，则由N个BCE组成的异构多核密码处理器，除m个异构核外，余下同构核数量N_{homo}表示如下：

$$N_{\text{homo}}=N-\sigma\cdot\sum_{i=1}^{m}\frac{1}{s_i} \tag{4}$$

(2)并行执行时间T_{p}. 密码任务的并行部分不是完全并行的，而是由多个不同并行度的并行段组成. 为更符合密码任务实际，将并行执行部分采取分段形式描述，并考虑同构核数量N_{homo}的限制. 假设密码任务并行部分被划分成P段，f_j表示第j个并行段，对应并行度用p_j表示. 任务并行部分执行时间可表示如下：

$$T_p=\sum_{j=1}^{P}\frac{f_j}{p_j}\cdot\left\lceil\frac{p_j}{N_{\text{homo}}}\right\rceil \tag{5}$$

其中，f_j/p_j表示第j个并行段的执行时间，特别地，当p_j=1时，等价于串行执行，且有$\sum_{i=1}^{m}q_i+\sum_{j=1}^{P}f_j=1$，表示整个密码任务由串行、并行任务组成；$\left\lceil\frac{p_j}{N_{\text{homo}}}\right\rceil$表示由于同构核数量资源限制，当并行度超过同构核数量时，执行时间会增加.

(3)数据准备时间$g(N)$. 整个数据准备时间由输入输出数据传输时间、核间通信时间、同步竞争等待时间三部分组成. 由于密码任务的数据操作特性，除密钥、参数的获取，发生同步竞争的场景较少，在整个数据准备时间中占比低，且对于给定的密码任务，同步竞争时间一般固定；数据传输时间与异构多核密码处理器的核数、密码任务数量相关，当任务量一定时，主要与BCE数量N成正比；核间通信时间由核数量、拓扑结构相关，为简化模型，这里假设异构多核密码处理器采用mesh结构、NoC通信方式，通信时间取决于一次传输消息个数、节点平均延迟、多核传输平均跳数. 为简化模型，模型中三种时间消耗统一用$g(N)$($0<g(N)<1$)表示，即数据准备时间占任务完成时间的比例.

(4)DVFS技术影响f_{DVFS}. f_{DVFS}表示动态电压频率调节技术对异构多核密码处理器的影响参数. 在性能模型上，主要表现于频率的变化. 频率Fre变化与密码任务的处理时间大小成反比，即频率越高，任务执行时间越少，其影响可表示如下(ρ表示比例参数)：

$$f_{\text{DVFS}}=\frac{\rho}{\text{Fre}} \tag{6}$$

由式(2)~(6)可得，异构多核密码处理器的密码任务完成总时间T_{N}为

$$\left.\begin{aligned}
&T_{\text{N}}=\frac{\rho}{\text{Fre}}\cdot\left(T_{\text{s}}+T_{\text{p}}\right)\cdot\left(1-g(N)\right)+g(N)\\
&T_{\text{s}}=\sum_{i=1}^{m}\left(r_i\cdot s_i\cdot q_i\right),\ r_i\in\{0,1\}\\
&T_{\text{p}}=\sum_{j=1}^{P}\frac{f_j}{p_j}\cdot\left\lceil\frac{p_j}{N_{\text{homo}}}\right\rceil\\
&N_{\text{homo}}=N-\sigma\cdot\sum_{i=1}^{m}1/s_i
\end{aligned}\right\} \tag{7}$$

所以异构多核密码处理器性能加速比如式(8)所示:

$$S_{\mathrm{N}}=\frac{1}{T_{\mathrm{N}}} \tag{8}$$

3.3 能耗模型建立

对N个BCE组成的异构多核密码处理器,设每个核根据是否执行密码任务将其状态分为空闲(idle)、活跃(active)两种. 对于能耗模型的建立,做如下假设.

(1)对单个BCE组成的同构核,设其活跃时功耗为1,其空闲时功耗为k_s($0<k_s<1$). 对同一个密码处理器核,当任务不同时,功耗会有差别. 考虑到此处假设的是瞬时功耗,为简化模型,分析能效变化趋势,所以用固定参数表示.

(2)对m种不同异构核,设active状态时,相较于同构核的功耗,用向量$\boldsymbol{E}=(e_1,e_2,\cdots,e_m)$表示异构核的功耗,$e_i$表示第$i$($1\leqslant i\leqslant m$)个异构核的功耗,且$1<e_i$,表示异构核功耗大于同构核. idle状态时,用向量$\boldsymbol{K}=(k_1,k_2,\cdots,k_m)$表示空闲状态相较于活跃状态的功耗,其中$0<k_i<1$($1\leqslant i\leqslant m$).

(3)数据准备时间消耗的平均功耗为e_{dp}. 根据上述假设,异构多核密码处理器消耗的总能量E_{N}可以用式(9)表示. 式(9)中,E_{s}表示密码任务串行部分执行时消耗的能量,E_{p}表示密码任务并行部分执行时消耗的能量,E_{DP}表示密码任务数据准备阶段消耗的能量.

$$E_{\mathrm{N}}=E_{\mathrm{s}}+E_{\mathrm{p}}+E_{\mathrm{DP}} \tag{9}$$

串行部分执行时消耗的能量E_{s}包括异构核active状态下执行串行密码任务能耗、异构核idle状态下能耗、同构核idle状态下能耗3部分,考虑数据准备时间和DVFS技术对时间影响间接导致的影响,可用式(10)表示:

$$\left.\begin{aligned}
&E_{\mathrm{s}}=\left(E_{\mathrm{sactive}}+E_{\mathrm{sidle}}\right)\frac{\rho\cdot(1-g(N))}{\mathrm{Fre}}\\
&E_{\mathrm{sactive}}=\sum_{i=1}^{m}e_i\cdot r_i\cdot s_i\cdot q_i\\
&E_{\mathrm{sidle}}=T_{\mathrm{s}}\cdot\sum_{i=1}^{m}\left(e_i\cdot k_i\cdot(1-r_i)\right)+\sum_{i=1}^{m}\left(e_i\cdot k_i\cdot r_i\cdot\left(T_{\mathrm{s}}-s_i\cdot q_i\right)\right)+N_{\mathrm{homo}}\cdot k_{\mathrm{s}}\cdot T_{\mathrm{s}}
\end{aligned}\right\} \tag{10}$$

并行部分执行时消耗的能量E_{p}包括并行部分执行时异构核idle状态的能耗、并行部分执行时同构核idle状态的能耗、并行部分执行时同构核active状态的能耗(假设单位时间能耗为1),考虑数据准备时间和DVFS技术的间接影响,可用式(11)表示:

$$\left.\begin{aligned}
&E_{\mathrm{p}}=\left(E_{\mathrm{pidle}}+E_{\mathrm{pactive}}\right)\frac{\rho\cdot\left(1-g(N)\right)}{\mathrm{Fre}}\\
&E_{\mathrm{pactive}}=\sum_{j=1}^{P}f_j\\
&E_{\mathrm{pidle}}=T_{\mathrm{p}}\cdot\sum_{i=1}^{m}e_i\cdot k_i+\sum_{j=1}^{P}\left(\frac{f_j}{p_j}\left(\left\lceil\frac{p_j}{N_{\mathrm{homo}}}\right\rceil N_{\mathrm{homo}}-p_j\right)k_{\mathrm{s}}\right)
\end{aligned}\right\} \tag{11}$$

数据准备阶段消耗的能量E_{DP}可表示如下:

$$E_{\mathrm{DP}}=e_{\mathrm{dp}}\cdot g(N) \tag{12}$$

式(10)~(12)仅考虑DVFS技术对密码任务执行时间的影响,进而影响整体能耗的情况. 实际上,电压与频率的改变本身也会影响能耗的大小,对CMOS电路,其功率一般表示如下:

$$P=\alpha\cdot C\cdot V^2\cdot f_{\mathrm{clk}}+V\cdot I_{\mathrm{short}}+V\cdot I_{\mathrm{leakage}} \tag{13}$$

其中,第一项表示动态功耗,第二项和第三项分别表示短路功耗和泄漏功耗,即静态功耗. 在电路结构和处理任务确定时,功率大小主要受频率和电压的影响. 动态功耗与$V^2\cdot f_{\mathrm{clk}}$成正比,静态功耗与$V$成正比. 而$V$与$f_{\mathrm{clk}}$之间是相关联的,一般来说一个电压值对应一个可支持的最大频率范围,电压越大,能支持的频率越大,但到达某一值后,提升电压也无法再提高频率,这与具体电路参数有关. 电压与频率的关系,可以将动态功耗中的影响统一到频率变量上,静态功耗则主要取决于一固定电压值. 考虑DVFS技术对功耗直接影响时,结合密码处理器核的active和idle状态,可以认为在active时动态功耗占主要部分,在idle时静态功耗占主要部分,即DVFS技术对功耗的直接影响可用函数Dyn(Fre)和函数Sta(V)表示如下:

$$\left.\begin{aligned}
&\mathrm{Dyn}(\mathrm{Fre})=\gamma\cdot\mathrm{Fre}^3\\
&\mathrm{Sta}(V)=\lambda\cdot V
\end{aligned}\right\} \tag{14}$$

其中,γ为异构多核密码处理器电路及密码任务相关的特征参数,λ表示DVFS技术对电压的管理程度,理想情况下,$\lambda=0$表示DVFS技术管理电压使静态功耗消耗为0. 一个固定电压对应一固定的Sta影响和一定范围的Dyn影响. 由式(10)~(12)和式(14)可得,考虑DVFS技术对功耗的直接影响后,对应各部分功耗如式(15)所示:

$$\left.\begin{aligned}
&E_{\mathrm{s}}=\left(\mathrm{Dyn}\cdot E_{\mathrm{sactive}}+\mathrm{Sta}\cdot E_{\mathrm{sidle}}\right)\frac{\rho\left(1-g(N)\right)}{\mathrm{Fre}}\\
&E_{\mathrm{p}}=\left(\mathrm{Dyn}\cdot E_{\mathrm{pactive}}+\mathrm{Sta}\cdot E_{\mathrm{pidle}}\right)\frac{\rho\left(1-g(N)\right)}{\mathrm{Fre}}\\
&E_{\mathrm{DP}}=\mathrm{Dyn}\cdot e_{\mathrm{dp}}\cdot g(N)
\end{aligned}\right\} \tag{15}$$

3.4 能效模型建立

根据上述性能模型与功耗模型,可以得到异构多核密码处理器的平均功耗W_{N}如式(16)所示:

$$W_{\mathrm{N}}=\frac{E_{\mathrm{N}}}{T_{\mathrm{N}}} \tag{16}$$

在前述假设单个同构核执行密码任务性能为1的前提下，异构多核密码处理器的性能加速比为$1/T_{\mathrm{N}}$，则由式(2)、式(9)、式(16)可得异构多核密码处理器的能效如式(17)所示：

$$\frac{\mathrm{Perf}}{W}=\frac{\frac{1}{T_{\mathrm{N}}}}{W_{N\mathrm{N}}}=\frac{1}{E_{\mathrm{N}}} \tag{17}$$

式(17)表示的能效值以每W能耗得到的性能为单位，表示单位能量获得的性能，实际比较处理器能效值时，用每焦耳能耗得到的性能表示单位能量在单位时间内获得的性能，同时限制了时间与能耗，即能量延迟积的倒数[18]，更符合对能效的描述，之后分析均用这一指标，即由式(9)、式(17)可得能效值如式(18)所示：

$$\frac{\mathrm{Perf}}{J}=\frac{1}{E_{\mathrm{N}}\cdot T_{\mathrm{N}}} \tag{18}$$

4 密码处理器高能效设计空间探索

该节对提出的能效模型进行分析，通过分析模型中各类参数对能效值的影响，对高能效异构多核密码处理器的设计空间进行搜索，发掘多核架构对能效值提升的潜力，为高能效多核密码处理器设计提供建议．同时通过对多核密码处理器芯片板级实测，验证了提出模型的有效性．模型假设单个BCE同构核完成密码任务的性能为1，功耗为1，因此能效值也为1，作为评价多核架构下能效值变化的参考量．建立的能效模型参数具体可以分为多核架构、密码任务特征、能效影响因素这3类．对多核架构类，模型中的N，m，$\boldsymbol{S}$这3个参数决定多核的架构，用于分析架构对能效值大小的影响．对密码任务特征类，参数$\boldsymbol{Q}$，$\boldsymbol{R}$，f_j，p_j分别表示密码任务串并行部分的划分、占比、并行度，这些参数描述了密码任务的特征，用于分析不同密码任务应用场景下的能效值变化．能效影响因素考虑数据准备时间开销、DVFS技术增益正反两方面．在数据准备时间消耗上，统一用函数$g(N)$表示；DVFS技术主要考虑当电压和频率动态可调节时，对能效值的影响，在模型中由V和Fre这2个变量决定．

4.1 异构多核架构参数分析

图2中异构多核密码处理器架构由3个异构核加数量可变的同构核组成，简记为架构1．3个异构核分别由8个、4个、2个等价BCE组成，其性能$\boldsymbol{S}$=(0.125，0.25，0.5)，表示串行密码任务在异构核上执行消耗更少的时间．处理的密码任务1串行部分$\boldsymbol{Q}$=(0，0.1，0.1)，并行部分为f_j=(0.2，0.2，0.2，0.2)，对应并行度为2，4，4，2．

从图中可以看到，随着组成异构多核密码处理器总体BCE数量N的增加，能效值变化趋势是先增加、后不断减小，且在BCE数为18时达到最大．在N较小时，同构核数量小于密码任务1的最大并行度，并行部分任务的性能受到限制，且此时同构核的能耗还比较小，在性能与功耗权衡中，性能的不足占主要因素．随着同构核数量增大，任务1并行部分性能得到提升，异构多核密码处理器架构的能效值逐渐上升，当同构核数量达到4时，能够满足密码任务1的最大并行度，能效值也达到最大．之后再增加同构核数量，性能已经无法提升，但同构核增加会导致idle状态下功耗的增加，此时随着N不断增加，能效值会一直下降．

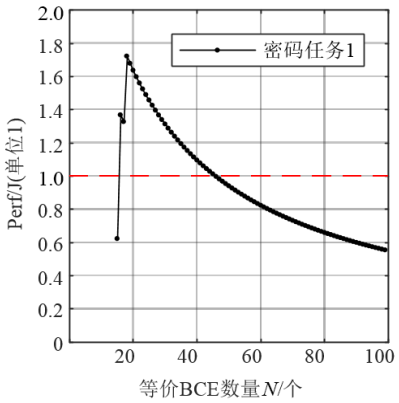


图2 任务1-架构1下N对能效值影响

为进一步研究能效最大值的取得点，对密码任务1、任务2、任务3、任务4在架构1下用MATLAB进行仿真，得到如图3所示的结果．

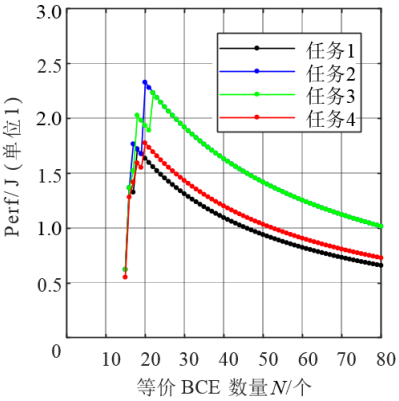


图3 架构1-多种任务下N对能效值影响

从图中可看出，架构1下，4种任务能效值曲线总体变化趋势都是先增大后减小．任务1、任务2、任务3、任务4取最大能效值分别在N=18，N=20，N=22，N=20时，即同构核数量与密码任务的最大并行度相等时．这表明在固定异构核数量情况下，异构多核密码处理器在同构核数量与执行任务最大并行度相等时取得最大能效值．同时注意到图2、图3中各密码任务在取得最大能效值之前，有一个阶段会暂时下降．通过分析发现，

这与密码任务的并行度划分有关. 以任务1为例,当同构核数量小于2时,N增加,性能增加,能效值也增加. 当同构核数量大于2,且小于最大并行度4时,增加N,此时同构核数量不足,无法通过增加并行性提升性能,但另一方面多的空闲核导致功耗增加,因此能效值会出现一个下降阶段. 在密码任务应用场景2、场景3、场景4均不同程度地出现了这种情况,本质上是因为密码任务并行部分各分段的并行度差异. 观察密码特征相似的任务1、任务4两条曲线,在相同N时,任务4的能效值要高于任务1. 进一步比较两者的密码特征差异,任务4的最大并行度要略高于任务1,且任务4的并行部分占比更高. 这表明对于异构多核密码处理器,密码任务并行部分占比和密码任务最大并行度是影响最大能效值的关键因素.

对模型进行仿真时发现,同构、异构核的空闲/活跃能耗比参数k_s和$\boldsymbol{K}$对能效值结果变化较大. 为探究这种情况,在架构1、任务1场景下,对k_s和$\boldsymbol{K}$分别取0.2,0.1,0.05,0.01这4个值进行仿真,得到如图4所示的结果. 从图中可以看到,随着k_s和$\boldsymbol{K}$取值的减小,曲线对应的能效值有较大的提升,相比于取0.2时的最大能效值,取0.1,0.05,0.01时最大能效值分别提升了1.3倍、1.6倍、1.9倍. 且从图4中可以看到,在下降阶段,k_s和$\boldsymbol{K}$取值越大,曲线斜率越小,即下降速度越慢. 这是因为活跃/空闲能耗占比越小,空闲状态的能耗就越少,N值增大导致空闲同构核增加的能耗开销变小,能效值下降更慢(曲线斜率更小). 这个现象一方面表明多核架构中处理器核活跃/空闲状态功耗比值对能效影响的重要性,另一方面也暗示引入DVFS、时钟门控等功耗管理技术降低空闲核的能耗对能效值提升具有积极影响.

对异构核类型与数量固定情况下能效变化进行了分析,但实际模型中异构核数量与类型是可变的. 图5为4种密码任务下变化异构核数对能效值的影响,图中X轴为总BCE数量,Y轴为异构核数,Z轴为能效值.

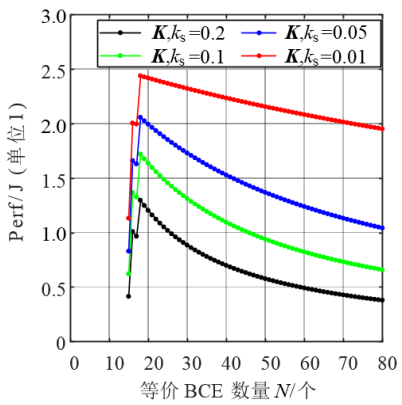


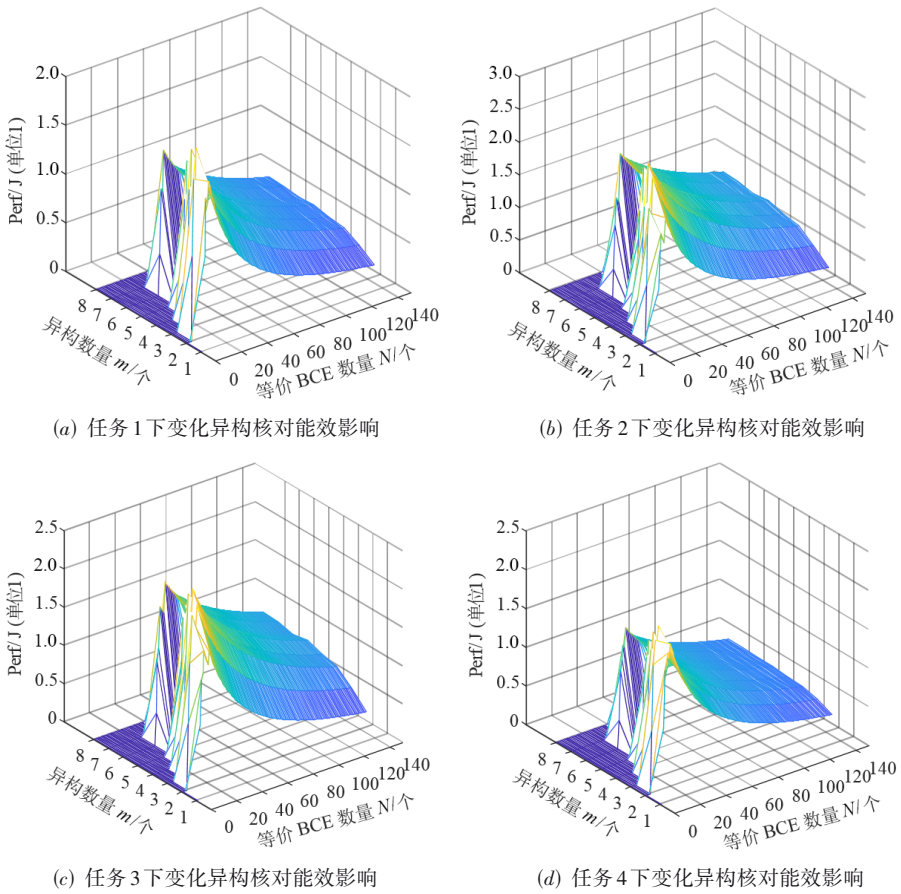
图4　不同k_s和$\boldsymbol{K}$对能效值影响

图5(a)表示改变异构多核密码处理器的异构、同构核数量,即不同核数架构下执行任务1的能效值变化. 从图中可以看到,当固定取某一异构核数m时,能效值随着BCE部分变化趋势同之前分析一致,如固定m为3时,变化曲线中N=16时能效值最大,即与密码任务1的最大并行度相关. 但观察m变化时能效变化趋势可以看到,当N固定时,伴着m的变化,能效值有先增大后减小的趋势. 这是因为当m=1时,表示一个异构加多个同构核架构,但这种方式并不一定能完全适应密码任务串行特征,能效值未取得最大值. 但当m过大,即异构核过多时,虽然能够满足密码任务串行特征,但空闲异构核过多会导致能效值下降,因此最高能效值一般取中间某一值. 图5(a)中,对于密码任务1,当异构核数量m=2,N=8,即由2个异构核(BCE数分别为2,2)、4个同构核组成异构多核密码处理器时其能效值最大,对应值为1.962.

图5(b)(c)和(d)分别对应密码任务2、任务3、任务4,其变化趋势与图5(a)类似. 图5(b)中,密码任务2在异构核数量m=3,N=18,即由3个异构核(BCE数分别为4,4,4)、6个同构核组成的架构下能效值最大,为2.518. 图5(c)中,密码任务3在m=3,N=20,即由3个异构核(BCE数分别为4,4,4)、8个同构核组成的架构下能效值最大,为2.422. 图5(d)中,密码任务4在m=2,N=10,即由2个异构核(BCE数分别为2,2)、6个同构核组成的架构下能效值最大,为2.131. 当m=1时,本质就是采用完全同构核的组织方式,从图5(a)~(d)这4个图中可以观察到,其能效值最大都不是在m=1处取得,这表明异构核架构在能效提升上要优于同构架构,这是因为异构核优化密码任务的串行部分性能,有增大能效值的潜力. 同时观察到,对于图5(a)(b)和(c)执行的密码任务中串行部分占比相同,但不同架构执行最大能效值仍有差异. 这表明尽管异构核方式通过优化密码任务串行部分提升能效,但不同架构提升效果是有差异的,这一架构需要结合具体密码任务. 该文建立的模型可以用于辅助设计高能效多核密码处理器时,确定多核架构组织异构核、同构核的核数量配置.

4.2　能效模型影响因素分析

除异构多核架构参数外,模型还考虑了数据准备时间消耗、DVFS技术对多核密码处理器能效值的影响. 为重点研究分析影响因素,下述分析均在密码任务1、异构架构1条件下进行. 假设多核密码处理器中数据准备平均能耗e_{dp}为1,实际数据准备功耗与密码任务、多核架构相关,这里假设其与活跃时同构核功耗相同,即都为1. 分别对数据准备消耗占比$g(N)$取不同值,得到能效变化如图6(a)所示. 随着$g(N)$(图中用gn



(a) 任务1下变化异构核对能效影响　(b) 任务2下变化异构核对能效影响

(c) 任务3下变化异构核对能效影响　(d) 任务4下变化异构核对能效影响

图5　不同任务下变化异构核对能效值影响

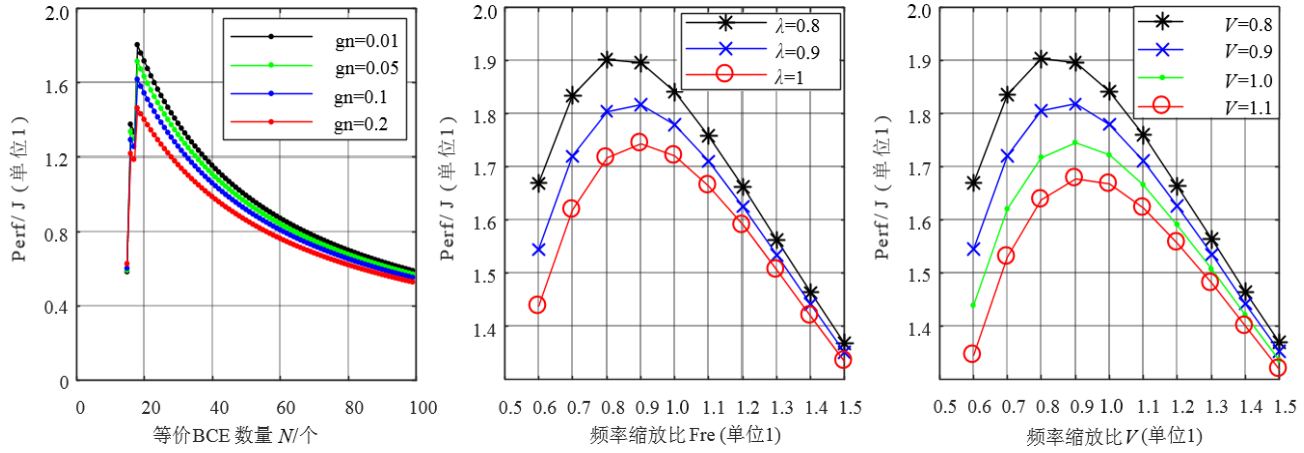
表示)占比的减小,能效值变化曲线图位置逐渐升高,即能效值变大. 观察4条曲线的位置情况可以看到,当$g(N)$由0.2减小到0.1时,曲线上升幅度要大于由0.05减小到0.01,这说明尽管前者减小到1/2,后者是减小到1/5,但当$g(N)$较小时,其变化对能效值的影响在减弱,这表明对异构多核密码处理器,若能将数据准备时间占比控制到一个较小量级,对能效值影响较小,即$g(N)$的影响不是呈线性关系的,而是在一定限度内. 观察4条曲线的起始点,注意到占比较大的$g(N)$=0.2能效值反而要比占比小的稍大. 这是因为该点同构核数只有1个,尽管数据准备时间占比小,因同构核数量为1,数据准备时间占比小,其计算时间占比大,但计算时间由于并行度无法充分发挥,其消耗时间过大,反而使总体性能下降,能效值降低.

图6(b)和(c)为DVFS技术对能效值的影响变化趋势. 图(b)为固定DVFS技术的电压缩放参数V=1,改变静态功耗影响Sta中的参数λ取值得到的变化曲线. 当固定电压时,随着频率变量Fre的变化,3条曲线的能效变化趋势均是先增大后减小. 当Fre过小时,异构多核密码处理器的性能下降过多,导致能效值下降;当Fre过大时,会增加动态功耗的消耗,也会引起能效值的降低,因此其能效值取最大是在Fre的中间某一值. 值得注意的是,当Fre=1,λ=1,V=1时,表示不考虑DVFS技术影响,此时对应的能效值正好是前述不考虑DVFS技术的大小. 另外,观察3条曲线在不同λ取值下的变化. λ表示DVFS技术对空闲核电压管理的程度,λ越小,管理效果越好. 图6(b)中3条曲线的高度位置表明,好的DVFS技术通过减小空闲核的功耗,可以较大地提升异构多核密码处理器的能效值.

图6(c)表示在不同固定电压缩放值V下,能效值随着频率缩放Fre的变化趋势. V>1表示为提供更高频率,电压值超过正常值;V<1表示当所需频率较低时,可降低电压值到正常值以下. 对比图中4条曲线位置高度,随着V值的增大,曲线位置是不断下降的,这个结果表明DVFS技术在保证频率要求前提下,为获得更高能效应尽可能调低电压,同时适当的调低频率有利于能效值的提升. 图6(b)和(c)中的曲线均是在Fre=0.9左右位置取得最大值,即对密码任务1,频率缩放到90%左右运行能取得更好的能效值.

4.3　异构多核密码处理器多任务能效分析

为进一步探索异构多核密码处理器对能效的提升

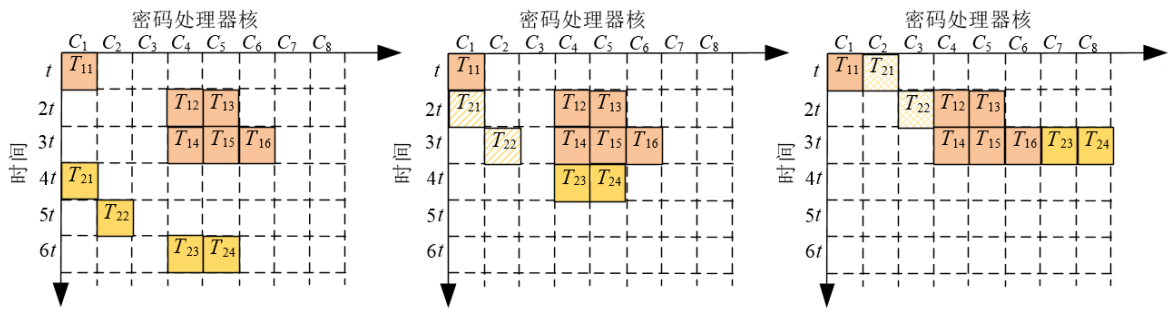


(a) 数据准备消耗影响　(b) DVFS技术参数λ影响(固定V=1)　(c) DVFS技术电压V影响

图6　数据准备时间、DVFS技术对能效值影响

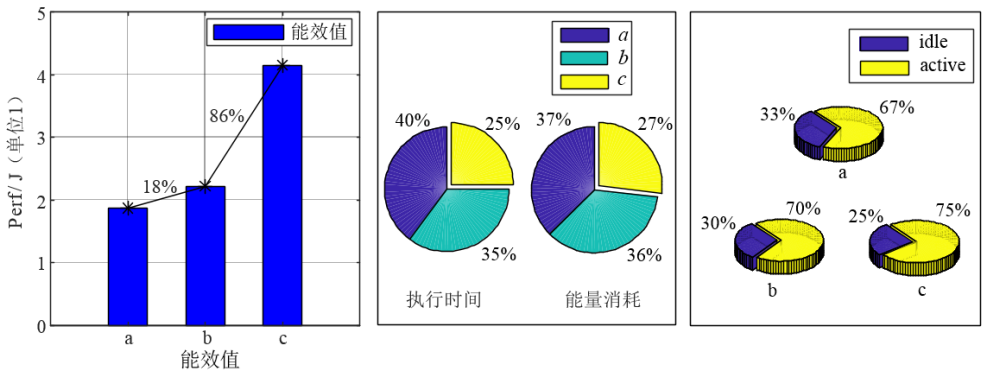
潜力,分析在异构多核密码处理器硬件构架固定条件下,多密码任务场景调度执行方式(顺序执行、流水执行、并发加流水执行)对能效值的影响. 在已构建的能效模型基础上:假设执行两个互相无数据依赖关系的任务,用Task_1和Task_2表示,T_{ij}表示第i个密码任务的第j个任务执行分段(可能为串行段或并行段);假设异构多核密码处理器架构由8个核组成,用向量集$\boldsymbol{C}=(C_1,C_2,C_3,C_4,C_5,C_6,C_7,C_8)$表示,$C_1,C_2,C_3$为执行串行任务的异构核,$C_4$到$C_8$为5个同构核;不考虑数据准备时间与DVFS技术的影响,即$g(N)$为0,DVFS相关参数为1. 密码任务Task_1和Task_2在上述假设的异构多核密码处理器上顺序执行、流水执行、并发加流水执行可用图7表示. 图中任务Task_1被划分成串行段T_{11}和2个并行段,并行度分别为2和3;任务Task_2被划分成串行段T_{21}和T_{22}和并行段T_{23}和T_{24},并行度为2.

图7(a)表示Task_1和Task_2按照正常的顺序方式在多核密码处理器(8个核)上执行. t时段,异构核C_1执行串行段T_{11};$2t$和$3t$时段同构核C_4,C_5,C_6执行并行段;$4t$和$5t$时段,2个不同类型的异构核C_1和C_2执行Task_2的串行段T_{21}和T_{22};$6t$时段由同构核C_4和C_5执行任务2的并行段T_{23}和T_{24}. 基于建立的能效模型,在多核处理器架构1(3个异构核加同构核)下对a,b,c这3种执行方式的能效值进行MATLAB仿真分析. 实际上通过模型可以得到其对应的能效表达式,这里直接给出仿真结果,如图8所示. 如图8(a)所示,相比2个任务串行执行,流水执行和流水加并行执行2种方式对能效值的提升分别为18%和86%. 这说明即使架构、密码任务相同,多密码任务不同的调度执行方式,异构多核密码处理器的能效值也会不同. 仿真分析结果表明流水、并发执行方式能够提升能效. 进一步分析能效值增加原因. 从图8(b)可以看到,3种不同方式执行密码任务的时间与能耗比例关系为$a>b>c$,即流水、并行两种方式通过提升性能、降低功耗的途径来改善能效值. 图8(c)表示3种执行方式下异核多核处理器的能耗分布. 串行执行时总能耗中67%为活跃时消耗,33%为空闲时消耗;流水执行时,70%为活跃消耗,30%为空闲消耗;流水加并行执行时,75%为活跃消耗,25%为空闲消耗. 结果表明,完成同样任务情况下,不同执行方式,通过提升核的利用效率,减少空闲状态消耗的能量,可以间接提升整个异构多核密码处理器的能效.



(a) 顺序执行　(b) 流水执行　(c) 流水加并发执行

图7　异构多核密码处理器多任务不同执行模型任务流图



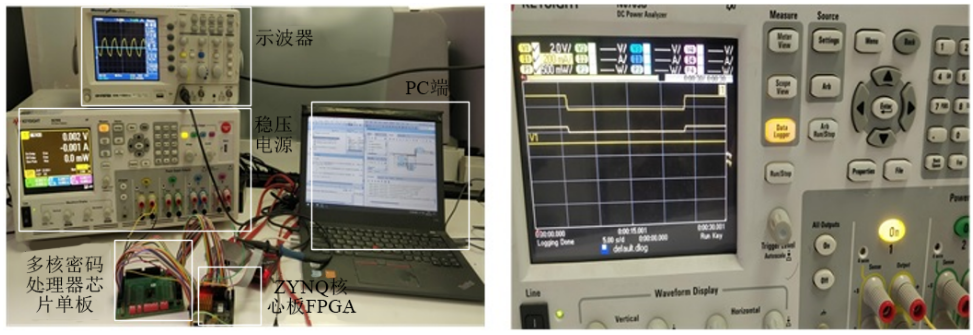
(*a*) 三种任务执行方式能效值　(*b*) 不同方式时间、能耗占比　(*c*) 不同方式空闲、活跃能耗占比

图8　3种执行方式对能效值影响

通过上述对各类参数分析，为适应高能效、异构性需求，异构多核密码处理器设计建议有：基于密码任务特征（最大并行度、串并特征），通过模型仿真确定异构、同构核数量；优化设计，将数据准备时间占比限制在10%以下；根据不同密码任务，执行频率相比正常频率可以缩放；多任务下调度执行采用并行、流水更有利于能效提升. 相较于其他基于Amdahl定律的多核处理器模型，该文提出的模型同时考虑性能、功耗两个方面建模；分析密码任务的串并特征，建立更符合实际的模型；考虑数据准备时间损失、DVFS技术增益正反两方面影响因素；在仿真中分析不同调度执行方式对能效变化影响. 该文通过对提出模型的分析，对各影响因素导致的能效值变化趋势进行研究，为高能效异构多核密码处理器设计提供有益的建议.

4.4　多核密码处理器芯片实测结果与分析

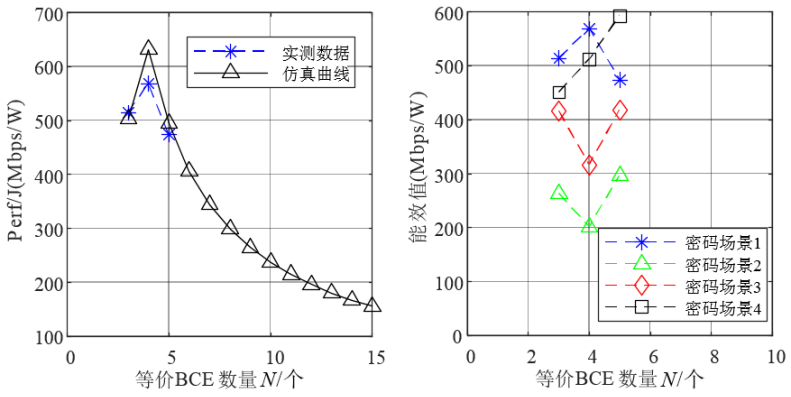
为验证所提模型的有效性，在现有多核密码处理器芯片上进行实际板级测试，将得到的实测数据与仿真结果进行分析对比，研究提出模型的有效性及不足. 多核密码处理器芯片板级实测环境如图9所示. 图9(*a*)为整个测试平台，由示波器、稳压电源、多核密码处理器芯片单板、ZYNQ系列FPGA、电脑PC端组成. 其中FPGA负责向多核密码处理器芯片发送指令与任务数据，密码处理器完成任务后将结果送回FPGA，由PC端进行结果数据比对，并计算性能. 图9(*b*)为稳压电源采样电压、电流示意图，通过采样密码处理器运算过程的电压、电流值，计算功耗，进而得到密码任务数据处理的能效值.



(*a*) 芯片板级测试平台　(*b*) 功耗测试

图9　多核密码处理器芯片能效板级测试

图9中多核密码处理器芯片有4个核心（含1个异构核），可通过钟控技术控制密码处理器核心是否工作，通过变化核心数得到实测如图10所示的核心数对能效值变化趋势的影响. 图10(*a*)为密码任务场景1下芯片实测能效值变化与模型仿真结果对比. 能效模型代入实测芯片的核数、同/异构核心性能、单核空闲/活跃能耗、密码任务串/并行比例分配等参数，得到图10(*a*)中的仿真曲线，密码任务场景1的最大并行度为2. 可以看到，尽管实测数据与仿真数据的数值大小有差距，但两者在变化趋势上是一致的，即均在同构核数为2时，达到能效最高值，之后随着同构核数量增加，能效值下降. 图10(*b*)为4种不同密码任务场景下芯片不同核心数的能效值变化趋势. 密码场景2、场景3并行部分最大并行度均为3，因此当同构核数为2时，增加的密码处理器核心无法带来性能提升，且功耗增大，因此能效值反而减小，但当同构核数达到3后，能效值又增大. 图10(*b*)中场景2、场景3的曲线高度不同，这是不同任务场景能效值不同导致的. 密码任务场景4的最大并



(a) 芯片实测与仿真对比　　(b) 不同场景下芯片实测能效变化

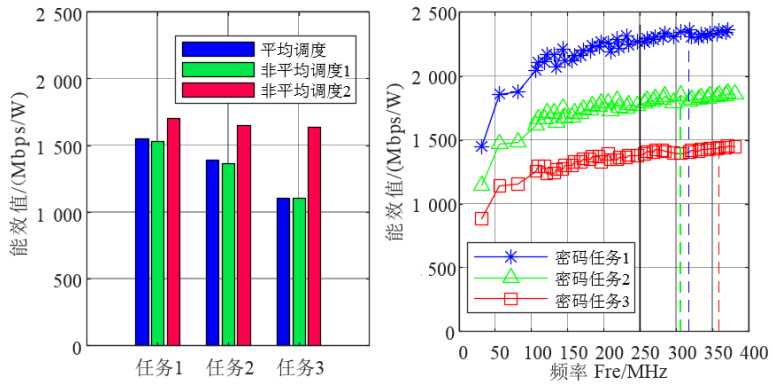
图10　多核密码处理器芯片不同核数实测能效值

行度也为3,但由于任务本身并行特点,每增加一个核心均能带来性能提升,因此随着同构核的增加,能效值逐渐上升. 实测分析的现象,在前述能效模型仿真中,也均能观察到.

对图10(*a*)的芯片实测数据与仿真结果数据利用相关性计算公式,得到其相关系数为0.93,表明仿真数据与实测数据有较强的相关性,在一定程度上反映了提出能效模型的有效性,同时也间接说明参数选取有其合理性存在. 通过以上测试可以分析得到,当已知同构单核、异构单核密码处理器的性能、功耗相关参数,以及对应的密码任务应用的串/并特征参数时,可以将这些参数代入到提出的异构多核密码处理器能效模型中,进行模型仿真,通过改变模型中的同构、异构核数,可以得到相应的仿真能效结果,建立起异构核类型与同构核数可变的多核密码处理器能效模型,并通过分析仿真结果,得到最佳的异构多核密码处理器的同构、异构核数量配置. 模型仿真中图5的结果即是模拟通过仿真得到最优能效值的同、异构核数配置的过程. 但同时,由于单个密码处理器芯片核心数量太少,实测分析中也存在数据支撑不够的问题,对相关性需要更多的数据计算. 后续将采用多个多核密码处理器芯片扩展形式,增大核心数量进行测试,进一步修正模型参数,提升模型的有效性.

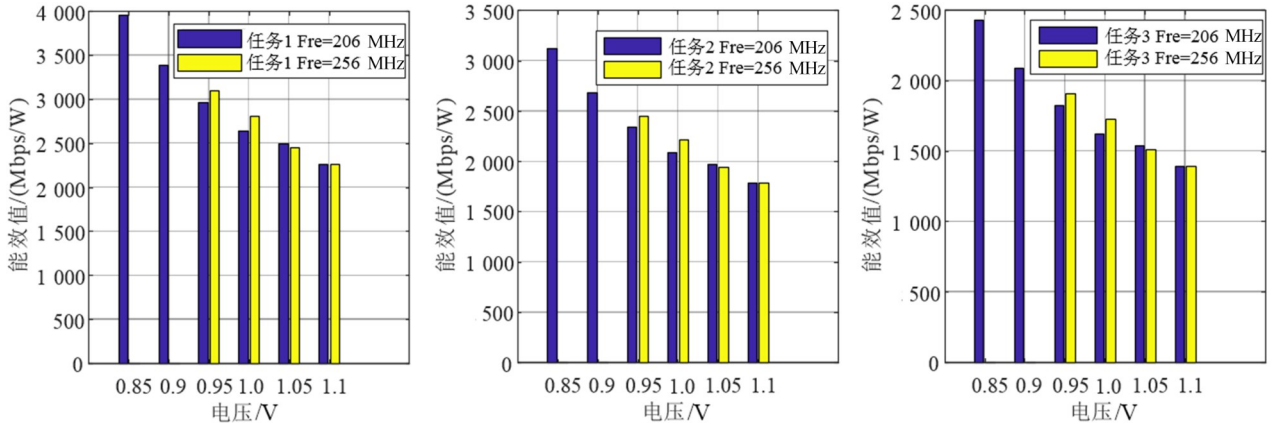
分析模型中考虑的数据准备时间(包括输入数据调度、核间通信等非计算时间)、DVFS技术频率电压变化等因素对异构多核密码处理器能效值的影响,实际测得数据如图11所示. 图11(*a*)表示输入相待量数据调度到各个密码处理器核的方式不同时(即数据准备时间$g(N)$不同),能效值的变化. 可以看到当$g(N)$占比过大时,不同数据准备时间对能效值也有较大影响,如对比“平均调度”方式,密码任务1、任务2、任务3在“非平均调度2”方式下的能效值分别提升了约10%,19%,48%,这说明异构多核密码处器设计中,应该尽量缩小数据准备时间的消耗,这也与前述影响因素的仿真结果相一致. 图11(*b*)表示不同密码任务下,不同频率芯片实测结果(正常工作频率为256 MHz). 从图中各实测散点数据连成的曲线可以看到,随着频率的增大,能效值会逐渐上升,但上升频率幅度(即斜率)减小,最终在某一点处达到一最大值(图中3条虚线处对应的点). 分析图11(*b*),相较于正常工作频率256 MHz,密码任务1、任务2、任务3分别在超过正常工作频率27.2%,22.4%,43.6%的点达到最大能效值. 对比发现,这个现象与前述模型仿真结果有很大不同,通过分析仿真模型中的参数发现,这是由于仿真分析中,对空闲时间处理器核心的能耗占比假设过于乐观,导致频率对能效值影响权重加大,仿真时假设空闲功耗为活跃时的20%,而实际芯片测试空闲功耗占比达60%左右. 图12为芯片实测DVFS技术的电压变化对异构多核密码处理器能效值影响,芯片正常工作电压1.1 V. 观察图12(*a*),可以看到在固定密码任务和频率下,电压值越低,功耗越小,进而能效值越高,且不同的工作频率,变化电压值得到的能效值提升幅度也不同. 但注意到,在工作频率206 MHz条件下,最低工作电压能降到0.85 V,但工作频率为256 MHz时,最低工作电压为0.95 V,即工作频率会受到电压的下限值的影响. 这与前述模型仿真分析得到的在频率固定下应尽可能采用最小的工作电压结论相一致. 注意到,对比图12(*a*)~(*c*)可以发现,不同密码任务,在同等降低电压情况下,尽管能效值不同,但得到的能效值提升幅度几乎相同. 如在工作频率206 MHz下,相比正常工作电压1.1 V,3种密码任务在0.85 V下得到的能效提升分别为75.03%,75.00%,74.56%,这说明通过改变电压提升异构多核密码处理器能效的方式与具体密码任务无明显相关性.

通过芯片板级实测,对提出的基于Amdahl定律的异构多核密码处理器能效模型的参数选取合理性、模



(*a*) 不同调度执行数据能效值 (*b*) 不同密码任务变化频率能效值

图11 变化数据调度及工作频率芯片实测能效值



(*a*) 密码任务1变化电压能效值 (*b*) 密码任务2变化电压能效值 (*c*) 密码任务3变化电压能效值

图12 变化电压值处理器能效变化

型有效性进行了分析与验证,同时对比模型仿真实验,对能效模型的影响因素也进行了芯片实测分析. 当前多核密码处理器模型研究主要有解析模型[10]、仿真模型[19]两类,本文属于解析模型类. 相较于同类基于Amdahl定律的多核密码处理器模型研究[10~14],本文提出的模型一方面在整体多核组织架构上,考虑更为复杂的异构核、同构核数量均可变化情况,且现有模型研究在能效模型方面研究较少;另一方面在影响因素上,一是考虑的密码任务串、并比例情况更符合实际,二是结合能效指标特点,引入了DVFS技术、数据准备时间占比对提出的能效模型进行修正,影响因素考虑更为全面. 相比仿真类模型,本文所提能效模型虽然在精准度上没有仿真模型精确,但一方面本文的重点是通过更高的抽象,分析异构多核密码处理器能效值的变化趋势,对模型具体数值精准度要求没有仿真模型那样高,重点以变化趋势准确为核心;另一方面,本文所提能效模型因为是确定的数学解析表示方式,计算时间复杂度只有$O(1)$,这远小于精确到具体电路的仿真模型的时间复杂度. 在实际应用中,可以用本文提出的能效模型,先进行高度抽象的分析,缩小设计空间范围,减小仿真时间,进而再采用更精确的仿真模型再次分析指导异构多核密码处理器的设计. 同时在具有电源管理机制的异构多核密码处理器中,可以利用本文提出的能效模型指导各个处理器核心的电源开关策略,进而面向不同的密码任务应用,采用不同的异构、同构核数配置,达到最佳的能效表现.

5 结束语

当前能效是异构多核密码处理器设计的重要衡量指标. 本文基于扩展Amdahl定律,构建了异构多核密码处理器的能效模型. 通过分析密码任务特征,着重考虑密码任务串、并执行实际情况及异构多核架构影响,并考虑数据准备时间、DVFS技术两方面因素对能效影响. 模型MATLAB仿真结果表明,多核密码处理器能效值提升主要从挖掘密码任务并行度以增加性能,提高密码任务与多核架构适应性以减少功耗两个方面努力. 高能效多核密码处理器的设计中,密

码任务最大并行度、串行任务划分占比是决定核架构的重要参数;数据准备时间占比、电压频率的选取能进一步提升能效值. 同时通过多核密码处理器芯片板级实测对所提能效模型的有效性进行验证. 但所提能效模型在数据准备时间细节方面研究不够深入,模型中部分假设过于简化,且实测因多核密码处理器芯片核数固定,实验数据量有待提升. 后续用模型指导实际异构多核密码处理器硬件设计后,利用多个芯片扩展构建更大处理器核数的平台,提取测试实际性能、功耗数据,并评估、修正模型,将是研究的重点.

参考文献

[1] 亓晋, 王微, 陈孟玺, 等. 工业互联网的概念、体系架构及关键技术[J]. 物联网学报, 2022, 6(2): 38-49.
QI J, WANG W, CHEN M X, et al. Concept, architecture and key technologies of industrial Internet[J]. Chinese Journal on Internet of Things, 2022, 6(2): 38-49. (in Chinese)

[2] 边缘计算产业联盟, 工业互联网产业联盟. 边缘计算安全白皮书[R]. 北京: 边缘计算产业联盟, 2019.
Edge Computing Consortium, Alliance of Industrial Internet. Edge Computing Security White Paper[R]. Beijing: Edge Computing Consortium, 2019. (in Chinese)

[3] BANERJEE U, WRIGHT A, JUVEKAR C, et al. An energy-efficient reconfigurable DTLS cryptographic engine for securing internet-of-things applications[J]. IEEE Journal of Solid-State Circuits, 2019, 54(8): 2339-2352.

[4] ZHANG Y Q, XU L, DONG Q, et al. Recryptor: A reconfigurable cryptographic cortex-M0 processor with In-memory and near-memory computing for IoT security[J]. IEEE Journal of Solid-State Circuits, 2018, 53(4): 995-1005.

[5] WANG W Z, HAN J, CHENG X, et al. An energy-efficient crypto-extension design for RISC-V[J]. Microelectronics Journal, 2021, 115: 105165.

[6] LIU S, ZOU B, ZHANG L M, et al. Heterogeneous CPU GPU-accelerated FDTD for scattering problems with dynamic load balancing[J]. IEEE Transactions on Antennas and Propagation, 2020, 68(9): 6734-6742.

[7] 何诗洋, 李晖, 李凤华. 面向格基密码体制的高效硬件实现研究综述[J]. 密码学报, 2021, 8(6): 1019-1038.
HE S Y, LI H, LI F H. A survey on high-efficiency hardware implementation for lattice-based cryptosystem[J]. Journal of Cryptologic Research, 2021, 8(6): 1019-1038. (in Chinese)

[8] 吴华麟, 陈文彬, 高崇志, 等. 同态签名研究综述[J]. 密码学报, 2021, 8(5): 758-777.
WU H L, CHEN W B, GAO C Z, et al. A survey of homomorphic signature schemes[J]. Journal of Cryptologic Research, 2021, 8(5): 758-777. (in Chinese)

[9] AMDAHL G M. Validity of the single processor approach to achieving large scale computing capabilities[C]//Proceedings of the April 18-20, 1967, Spring Joint Computer Conference. New York: ACM, 1967: 483-485.

[10] HILL M D, MARTY M R. Amdahl's law in the multicore era[J]. Computer, 2008, 41(7): 33-38.

[11] WOO D H, LEE H H S. Extending amdahl's law for energy-efficient computing in the many-core era[J]. Computer, 2008, 41(12): 24-31.

[12] MAROWKA A. Extending amdahl's law for heterogeneous computing[C]//2012 IEEE 10th International Symposium on Parallel and Distributed Processing with Applications. Piscataway: IEEE, 2012: 309-316.

[13] 冯晓, 戴紫彬, 李伟, 等. 基于Amdahl定律的多核密码处理器性能模型研究[J]. 电子与信息学报, 2016, 38(4): 827-833.
FENG X, DAI Z B, LI W, et al. Performance model of multicore crypto processor based on amdahl's law[J]. Journal of Electronics & Information Technology, 2016, 38(4): 827-833. (in Chinese)

[14] KIM M S, GAUDIOT J L, XIONG N X, et al. Energy efficiency of heterogeneous multicore system based on the enhanced Amdahl's law[J]. International Journal of High Performance Computing and Networking, 2018, 12 (3): 261.

[15] MENESES-VIVEROS A, PAREDES-LÓPEZ M, GITLER I. Amdahl's law extension for parallel program performance analysis on intel turbo-boost multicore processors [C]//International Conference on Supercomputing in Mexico. Cham: Springer, 2019: 87-96.

[16] RAFIEV A, AL-HAYANNI M A N, XIA F, et al. Speedup and power scaling models for heterogeneous many-core systems[J]. IEEE Transactions on Multi-Scale Computing Systems, 2018, 4(3): 436-449.

[17] POLLACK F J. New microarchitecture challenges in the coming generations of CMOS process technologies (keynote address)(abstract only)[C]//Proceedings of the 32nd Annual ACM/IEEE International Symposium on Microarchitecture. New York: ACM, 1999: DOI: 10.5555/320080.320082.

[18] GONZALEZ R, HOROWITZ M. Energy dissipation in

general purpose microprocessors[J]. IEEE Journal of Solid-State Circuits, 1996, 31(9): 1277-1284.

[19] LI S, AHN J H, BROCKMAN J, et al. McPAT 1.0: An integrated power, area, and timing modeling framework for multicore architectures[C]//2009 42nd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO). Piscataway: IEEE, 2010: 11057124.

作者简介

李 伟 男,1983年出生,天津人. 中国人民解放军战略支援部队信息工程大学教授. 主要研究方向为体系结构、安全芯片设计、集成电路技术. E-mail: try_1118@163.com

郎俊豪 男,1997年出生,重庆人. 中国人民解放军战略支援部队信息工程大学硕士研究生. 主要研究方向为智能化可重构芯片电路与架构.

E-mail: langjunhao2022@163.com