# 可重构计算密码处理器

刘雷波 王 博 魏少军 著

科学出版社

# 可重构计算密码处理器

刘雷波　王　博　魏少军　著

科学出版社

北京

## 内 容 简 介

本书主要介绍基于可重构计算技术的密码处理器系统设计方法，包括密码算法的动态重构实现特性分析、处理器系统结构设计与软件编译技术，并以一款作者团队设计的可重构计算密码处理器 Anole 为例讲解具体实现方案。在此基础上，本书重点讨论利用可重构计算形式的局部动态重构特性与阵列式处理架构提升密码处理器抗物理攻击安全性的设计方法，展望可重构计算密码处理器技术的未来发展。

本书适合电子科学与技术、密码科学、网络与信息安全、计算机科学与技术等专业的科研人员、研究生，以及工程师阅读学习。

**图书在版编目(CIP)数据**

可重构计算密码处理器/刘雷波，王博，魏少军著. —北京：科学出版社，2018.2

ISBN 978-7-03-054244-1

Ⅰ. 可… Ⅱ. ①刘… ②王… ③魏… Ⅲ. 加密系统 Ⅳ. TN918.4

中国版本图书馆 CIP 数据核字(2017)第 211294 号

责任编辑：魏英杰 / 责任校对：桂伟利

责任印制：师艳茹 / 封面设计：陈 敬

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京通州皇家印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2018 年 2 月第 一 版 开本：720×1000 1/16

2018 年 2 月第一次印刷 印张：22 彩插 6

字数：443 000

**定价：160.00 元**

（如有印装质量问题，我社负责调换）

# 序

可重构计算密码处理器是实现加解密算法的理想硬件载体之一。相对传统的密码处理器，可重构计算密码处理器能同时满足密码应用对高安全性、高能效性和高灵活性的要求。在安全性方面，动态可重构计算架构的功能不是单纯由硬件或者软件决定的，而是借助软硬件双编程动态定义。断电后具有“白片”特性，故难以通过侵入式攻击来获取密码算法。同时，动态可重构计算架构的执行模型具有专用性和不确定性，很难通过行为建模进行功耗、故障和电磁等侧信道攻击。因此，动态可重构计算架构对物理攻击的安全性较高。在性能和功耗方面，动态可重构计算架构主要采用空间并行化的方式进行运算，与密码算法的特性非常吻合，其能量效率（即性能功耗比）较高。在功能灵活性上，可重构计算架构能在运行中实时改变其硬件功能以适应不同的密码算法与执行模式，灵活性也非常好。随着近年来物理攻击手段的不断发展，即使密码算法的安全性做得很好，攻击者仍然可以从底层的密码处理器入手，通过侵入式或非侵入式的物理攻击手段窃取关键信息。正因为在对抗物理攻击上存在突出优势，可重构计算密码处理器已逐渐成为密码芯片的热点研究方向，密码领域的顶级会议和期刊上近年来有大量相关成果涌现。

传统密码处理器主要分成专用集成电路（ASIC）和指令集结构处理器（ISAP）两种。前者存在明显的安全性和灵活性缺陷。通过反向解剖 ASIC 芯片，攻击者可以破解其电路实现的密码算法，窃取其处理的秘密信息。此外，ASIC 芯片只能实现特定密码算法，几乎不具有功能灵活性，难以满足快速发展的应用需求。指令集结构处理器亦存在安全性问题。因为其系统执行过程容易进行建模，所以容易受到非侵入式的侧信道攻击。同时，指令集结构处理器的能效已经很难满足现在的实际应用需求。可重构计算密码处理器芯片很好地解决了这些棘手的问题，并已逐渐进入实用阶段。所以，可重构计算密码处理器将是未来密码处理器研究和实践都极有希望的方向。

刘雷波及其团队是国内可重构计算密码处理器研究领域的佼佼者，这得益于该团队在可重构计算领域的长期研究积累。刘雷波所在的清华微电子所团队在“十一五”和“十二五”期间完成了 2 个可重构计算方向的 863 重点项目，并获得 2015 年国家技术发明奖二等奖。该团队在相关领域的顶级会议和期刊上发表了一系列有影响力的学术论文，出版了学术著作《可重构计算》，相关专利还获得了 2015 年国家专利金奖，引领着国内在可重构计算领域的前沿研究。在将可重构计算技术应用到密码领域方面，该团队近年来也进行了卓有成效的开拓性研究工作，

提出利用动态重构特性提高密码处理器安全性、灵活性和能量效率的关键技术，包括基于时空随机化动态重构的抗故障和电磁攻击的方法、利用可重构计算架构生成物理不可克隆函数的技术、利用改进型 Benes 网络抗故障攻击的技术等。这些技术的新颖性、领先性和有效性给我留下深刻印象。

该书写作严谨、条理清晰、内容创新、观点独到，既对密码处理器的基础知识和研究现状进行了详细介绍，又对可重构计算密码处理器的设计方法和发展方向进行了讨论，是本领域不可多得的专著，因此我很愿意向读者推荐该书。

2017 年 6 月于北京

# 前　言

可重构计算密码处理器相比其他类型密码处理器，如用指令驱动处理器（ISAP）、可编程逻辑器件（FPGA）或专用集成电路（ASIC）实现的密码处理器，在安全性、能量效率（即性能功耗比）和功能灵活性上具有特殊的技术优势。

第一个技术优势体现在密码处理器的安全性上，原因有二。其一，可重构计算密码处理器内部的运算单元和互连模块虽然也可能是异构的，但仍旧非常规则：电路是规则的，布局布线也是规则的。通过观察硬件结构和电路组成难以获得算法信息。因此在流片过程中甚至在芯片遗失后，密码算法很难泄露。这被称为可重构计算密码处理器的"白片特性"，是很多应用单位非常关注的。其二，可重构计算密码处理器具有动态重构和局部重构特性，能在几个周期内改变运算功能和互连方式，重构时间在十几纳秒到几十纳秒的量级（FPGA 的重构时间在几百毫秒到几秒的量级），因此其抵御物理攻击的能力要远高于传统的密码处理器。这也是可重构计算密码处理器安全性相对较高的重要原因之一。这部分内容是本书的主要亮点之一，我们会进行非常详细的介绍。

第二个技术优势体现在，可重构计算密码处理器具有很高的能量效率，同时又能满足密码算法多样化、不断演进的功能灵活性需求。这主要归因于可重构计算处理器不仅支持软件编程，还支持硬件编程，能通过动态改变硬件来满足不断变化的软件需求。我们知道，在能量效率上最理想的是专用集成电路，然而这类电路不具有任何灵活性，硅实现后无法再修改功能，也无法再加入新功能，除非重新设计并再次流片。在芯片研制费用日益高启的今天，这种时间代价巨大、研制成本高昂的实现方式必将逐渐被市场淘汰。功能灵活性最好的是用指令驱动架构实现的密码处理器。这类密码处理器虽然能够运行目前、甚至未来绝大部分密码算法，但能量效率非常低，仅能达到专用集成电路的万分之一，有时甚至连万分之一都达不到，远远满足不了应用需求。除专用集成电路和指令驱动处理器外，还有一种更常见的密码处理器实现方式，就是用可编程逻辑器件来实现的方式。然而，这种实现方式在能量效率和功能灵活性上的表现仍旧不够理想。究其原因，从宏观上讲，FPGA 等可编程逻辑器件的灵活性太大（只要编程单元足够多，几乎就可以实现任何形式的数字逻辑），但灵活性的获得是以大幅牺牲能量效率和面积效率（即性能面积比）为代价的。密码运算虽然也有功能灵活性的需求，但其实并不需要这么强大的灵活性。为这些完全用不到的、额外的灵活性而不得不付出性能、功耗和面积代价是得不偿失的。微观角度来看，FPGA 等可编程逻辑器件的编程粒度太细（如

其核心运算单元查找表就是单比特粒度的),致使配置信息量太大、配置时间过长,无法实现真正意义上的动态重构和局部重构,从而致使能量效率和面积效率都无法进一步提高。虽然有些商用 FPGA 在产品宣传上也声称具备这种能力,但我们认为 FPGA 无法实现如可重构计算处理器一样的动态重构和部分重构,这是由 FPGA 的体系结构决定的。那些采用其他类型的技术,如用系统芯片技术(如 SoC)、可编程片上系统技术(如 SoPC、PSoC)、专用指令集处理器技术(如 ASIP)实现的密码处理器,无非是以上三种情况的组合或者变形。例如,SoC 实际上是指令驱动处理器跟专用集成电路的组合,SoPC 是可编程逻辑器件跟指令驱动处理器的组合,而 ASIP 是指令驱动处理器面向某个特定应用领域定制化的结果。这些密码处理器既继承了专用集成电路、指令驱动处理器和可编程逻辑器件的优点,又不可避免地沿袭了各自所固有的缺点,因此在能量效率和功能灵活性的表现仍旧不够好,未来也不可能有更大的提高。可重构计算密码处理器是为密码运算量身定制的处理器,硅实现后能够动态重构功能,算法上后向兼容,其功能灵活性正好能满足密码运算的要求,同时又不至于因为过于灵活而损失掉宝贵的能量效率和面积效率。我们的研究结果表明,在满足密码算法灵活性需求的前提下,可重构计算密码处理器的能量效率和面积效率能达到指令驱动处理器和可编程逻辑器件的 1～3 个数量级,甚至更大。为什么会有这样的结果?如何才能做到?这些内容我们在本书中也会有非常详细的介绍和分析。

本书共分 7 章:第 1 章介绍密码处理器的研究现状,分析传统的基于专用集成电路和指令集架构处理器的密码处理器在性能、功耗、灵活性和安全性等方面的优缺点,然后引出可重构计算的概念、可重构计算密码处理器的研究现状并对其进行分析。第 2 章对目前主流的密码算法进行分析,该分析以可重构计算架构为目标硬件平台,包括算法的共性逻辑提取、数据类型的特征提取、算法的并行性分析,从算法应用的角度出发初步讨论了硬件架构的设计。第 3 章从数据通路和控制器两个方面分析可重构计算密码处理器的硬件架构设计,介绍针对密码算法的硬件架构设计方法。第 4 章首先介绍可重构计算处理器的通用编译流程,然后讨论针对密码算法的特殊优化方法,最后用具体密码算法的编译实例进行了说明。第 5 章介绍我们团队设计的一款可重构计算密码处理器芯片,包括其基本架构、关键技术、集成开发工具以及芯片实现结果跟同类设计的对比。第 6 章介绍可重构计算密码处理器抵御物理攻击的新型技术,包括随机重构抗物理攻击技术、可重构阵列计算资源抗物理攻击技术。相比于将传统的抗攻击技术直接映射在可重构架构上,利用可重构特性的新型抗攻击技术可以通过资源复用减少安全性提升带来的性能、面积和功耗代价,还有望抵御未来的新型攻击方法。第 7 章对可重构计算密码处理器技术的发展方向进行展望,重点探讨硬件木马和全同态加密这两个方向。

本书凝聚了清华大学微电子所可重构计算密码处理器团队近7～8年的集体智慧。感谢王博、朱建峰、黄海、张能、黎奥、周卓泉、汪东星和王汉宁等同学和同事的参与，感谢魏少军教授对本书撰写工作的大力支持和指导，感谢我国信息安全领域著名专家蔡吉人院士百忙之中对本书的内容进行审阅并作序。最后，还要感谢我爱人和孩子们对我工作的理解和宽容，没有你们的支持，难以想象我可以完成这些工作，你们是我今后继续努力和前进的重要动力！

刘雷波

2017年8月于清华园

# 目　录

# 第1章 绪 论

密码处理器作为密码算法的实现载体，在信息安全应用中起到关键性作用。随着网络信息技术与集成电路技术的发展，密码处理器的应用需求不再局限于纯粹的计算性能。为了支持协议中尽量多的密码算法与执行模式，需要密码处理器有足够的灵活性；为了兼顾执行性能与处理器的功耗，能量效率（性能功耗比）相比纯粹的性能成为更加合理的需求指标；为了抵御近年来愈演愈烈的针对密码实现载体的物理攻击，安全性超越传统指标一跃成为密码处理器需求的重中之重。包括专用集成电路（application specific integrated circuit，ASIC）和指令集结构微处理器（instruction set architecture processor，ISAP）在内的传统密码处理器无法合理的兼顾灵活性、能量效率与安全性这三个需求指标，这不仅体现在 ASIC 缺乏灵活性而 ISAP 能量效率低下，更是由于 ASIC 与 ISAP 无法满足密码处理器在安全性上的苛刻需求。ISAP 利用基于指令的软件实现方式。由于指令的通用形式十分便于物理攻击的建模（如功耗攻击中功耗模型的建立），ISAP 的抗物理攻击能力相比硬件实现，普遍低 1～2 个数量级，无法适用于高安全性需求的应用场合。ASIC 的安全性问题主要体现在对于算法信息的泄漏上。在许多应用场合，密码算法本身需要进行保密（如军事、航天等特殊领域的非公开算法）。在采用 ASIC 实现时，若芯片丢失，攻击者通过逆向工程（reverse engineering）对芯片进行反向解剖就很可能破译其实现的保密算法。此外，在集成电路产业全球化大分工的背景下，芯片的流片过程一般需要外包给代工厂。ASIC 实现的保密算法极有可能因为不可信的代工厂通过反向解析设计文件而泄漏。作为一种新型的实现方法，可重构计算密码处理器不仅能够在灵活实现多种密码算法的同时兼顾较高的能量效率，而且在安全性上具有得天独厚的优势。一方面，可重构计算密码处理器采用配置流而非指令的驱动方式，其抗物理攻击安全性（physical attack resistance）远高于 ISAP 的软件实现。另一方面，可重构计算密码处理器具有基本相同的阵列结构，断电后对芯片的解剖并不会使算法信息泄漏，因此被认为具有“白片”的特性。总之，可重构计算密码处理器能够合理的权衡密码应用在灵活性、能量效率与安全性上的需求，是未来密码处理器中的一个重要而充满希望的发展方向。

## 1.1 信息安全与密码处理器

随着信息技术的快速发展和广泛应用，信息的传输、储存和交换方式都发生了巨大的改变，信息的沟通、获取和利用途径都极大丰富，为社会的发展、人们的生活都带来空前的便利。然而，随着信息技术在国家经济、政治、外交、国防和社会管理等领域发挥越来越关键的作用，信息安全也随之成为影响个人隐私与财产安全、社会金融与通信安全、国家政治与国防安全等各个方面的关键问题。

2013 年 3 月，韩国爆发历史上最大规模的黑客攻击，国内主流的银行、电视台计算机都被破坏，导致无法提供服务，大量资料被窃取，对韩国社会的稳定造成了巨大的影响。2015 年 1 月，有自称代表“伊斯兰国”的黑客入侵美国中央司令部的 YouTube 和推特账户，控制美国中央司令部推特账户长达 1 个小时，并把美国中央司令部的 logo 换成了“I love you ISIS”，对美国的国家安全和形象造成负面影响。2015 年 4 月，黑客组织 Cyber Caliphate 因不满法国总统奥朗德参加国际反恐行动，入侵了电视台的广播传输渠道，导致法国电视台 5 台遭到大规模网络攻击。2016 年 9 月，“iCloud 泄密”事件爆发，黑客通过攻击苹果 iCloud 云存储服务盗取了用户上传的照片，大量用户隐私数据在网上被曝光，对个人的隐私安全造成了很大威胁。信息安全已成为当今高度信息化的社会正常与稳定运行的重要基础，一旦信息安全出现问题，无论个人、团体，还是国家都会受到极大影响。2011 年美国制定了《网络空间国际战略》和《网络空间行动战略》，俄罗斯、英国、法国、德国、加拿大、澳大利亚、日本、韩国等，也先后制定了网络安全计划和组建了网络作战力量，以应对信息网络化带来的各种安全压力和挑战。我国也于 2014 年成立了中央网络安全和信息化领导小组。

信息安全具体指的是保护信息及信息系统不被未授权地访问、使用、泄漏、干扰、修改和损毁。其目的是保证信息的保密性、完整性和可用性[1]。图 1.1.1 展示了信息安全的不同层次。因为信息的基本载体包括设备、软件和通信等，所以最底层的信息安全就是保障设备和软件的安全，以及通信过程的安全，从而能够实现个人的信息安全，最终实现国家和社会的信息安全。密码算法是信息安全目标实现的基础，因为密码算法是确保信息保密性和完整性的必要条件。

① 信息的保密性指的是对信息的访问和公开进行授权限制。对称密码算法常常用于实现信息的保密性。对于数据量较小的信息，也常使用公钥密码实现信息的保密性。

② 信息的完整性具体指的是防止对信息的不恰当修改或破坏，确认信息的不可否认和真实性。信息的完整性主要通过杂凑算法和公钥密码来实现。

杂凑算法常常用于对消息生成校验码，确保信息未被毁坏，此外也可以用于实现消息认证码(message authentication code，MAC)，确保信息未被非授权修改。公钥密码常用于构造数字签名，保证信息的不可否认性。

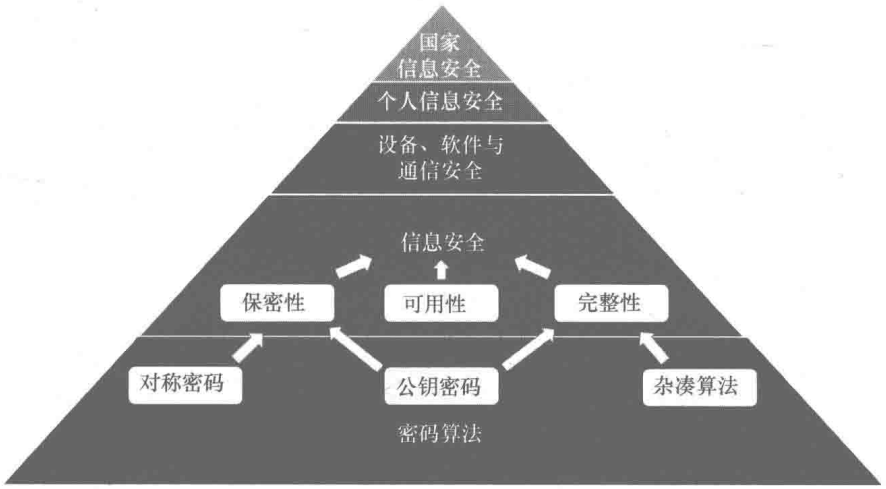


图 1.1.1 信息安全的不同层次

密码处理器是密码算法的实现载体，承担着信息安全基础设施的角色，已被广泛应用于物联网、互联网金融安全、保密通信和交通等不同领域，受到学术界和工业界的广泛关注和深入研究。

例如，在物联网中，物联网的体系和架构一般可分为感知层、网络层、应用层(图 1.1.2)，而信息安全问题存在于每个层次。感知层是物联网区别于互联网的特殊之处，它通过传感器采集数据，监测系统状态，主要使用射频识别(radio frequency identification，RFID)技术与网络层通信。这个通信过程如果不采取充分的安全措施就有可能受到干扰、屏蔽、窃取、伪装等攻击，产生信息安全问题。因此，安全性要求高的物联网设计都会在感知层增加密码芯片，对感知层设备的数据进行加解密，提供完整性校验机制，保证信息的安全。以心脏起搏器为例，安全公司 WhiteScope 的研究结果指出安装在人体的心律调节器及其外围系统存在大量的安全漏洞，对病患的安全造成严重的潜在威胁，需要大幅提高密码芯片及系统软件的安全性。因此，感知层的安全通信对密码处理器提出越来越高的需求。物联网的网络层和应用层与互联网类似，也需要借鉴 TCP/IP 网络、无线网络和移动通信网络等已有的信息安全和密码处理器技术。综上，密码处理器为物联网各个层面的信息安全提供了硬件基础。

又如，在金融领域，随着信息安全要求的不断提高，我国 2015 年起已经不再发行传统的磁条银行卡，取而代之的具有更高安全级别的芯片卡。金融卡密码处理

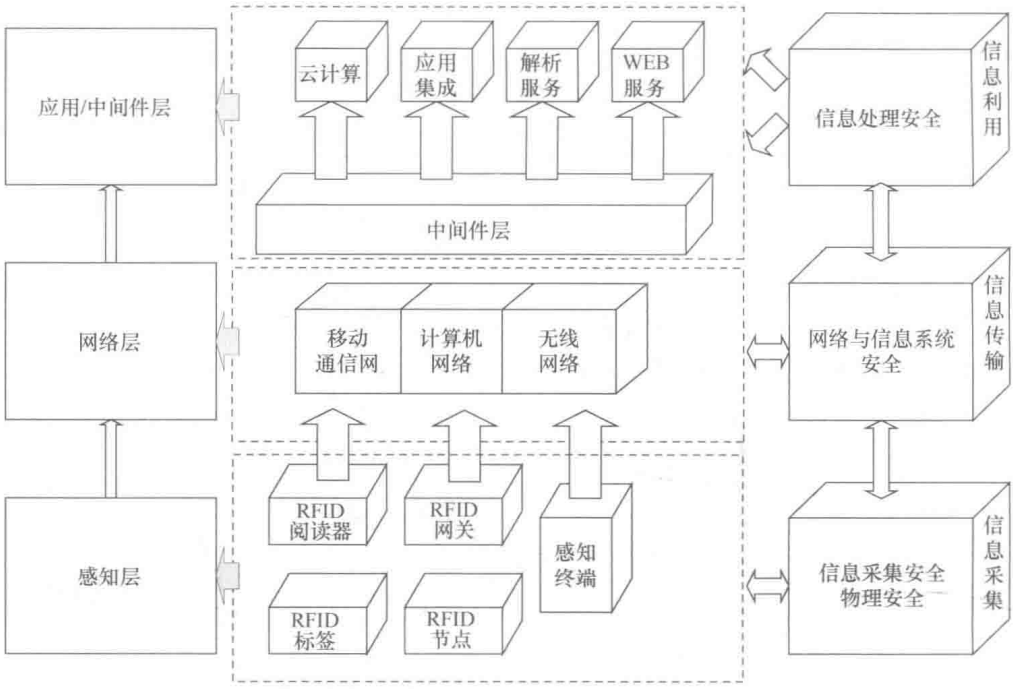


图 1.1.2　物联网三层体系架构图[2]

器实现了大量密码算法，如图 1.1.3 所示。可以看出，一个金融卡密码处理器中集成实现了分组密码算法 SM4、AES 和 3DES、杂凑算法 SM3 和 SHA1，以及公钥密码 SM2 和 RSA。集成多种密码算法的密码处理器可以有效保障金融卡的安全性。

本书的密码处理器指的是用于实现密码应用的各种类型的集成电路载体，它们需要在一定程度上针对密码算法进行优化，以满足密码应用的需求。密码处理器的具体形式可以分成 ASIC、ISAP 和可重构计算密码处理器三种。需要指出，本书提到的 ISAP 泛指所有基于指令集的处理器，包括通用微处理器(general purpose processor，GPP)、可编程数字信号处理器(digital signal processor，DSP)、图像处理单元(graphic processing unit，GPU)和专用指令集处理器(application specific instruction-set processor，ASIP)等。

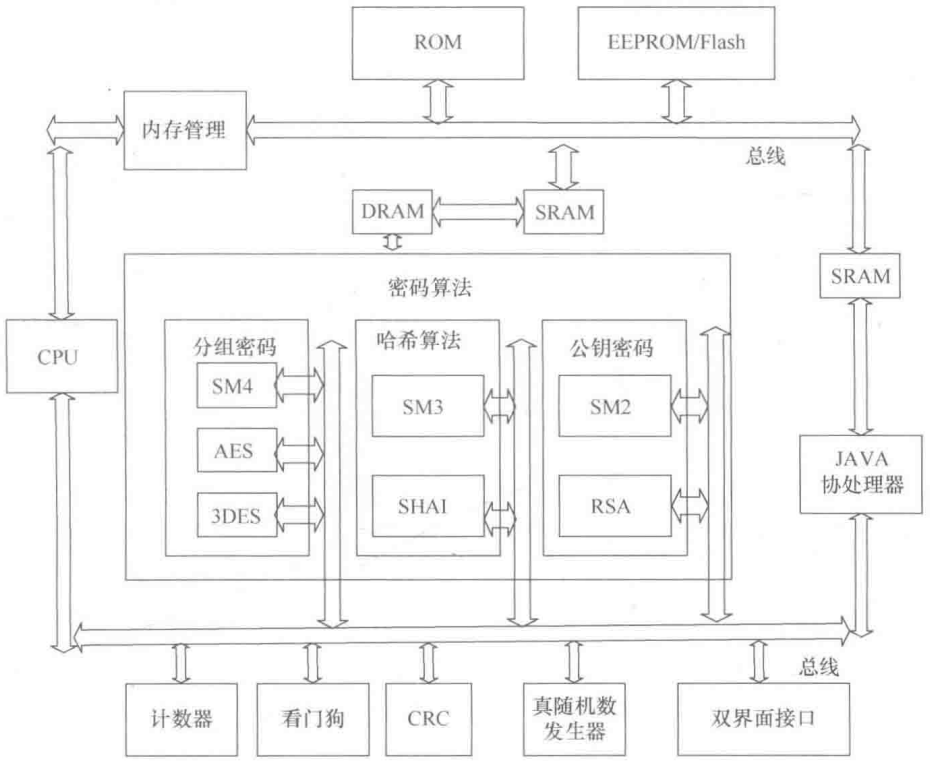


图 1.1.3 金融卡密码处理器中具有的密码算法[3]

## 1.2 密码处理器的应用需求挑战

日益发展的信息安全应用为密码处理器的设计带来前所未有的挑战。如图 1.2.1所示,密码处理器的应用需求可以归结为灵活性、能量效率与安全性。由于需求之间相互影响与制约,在设计过程中,需要合理的权衡各个需求间的关系。

1. 灵活性

密码处理器的主要处理对象是各类密码算法。密码算法按照功能可分为对称密码(symmetric cipher)、公钥密码(public-key cipher)(又称非对称密码)和杂凑算法(Hash function)。对称密码主要用于较大数据块或数据流的加密,其可进一步分为分组密码(block cipher)与序列密码(stream cipher)。公钥密码主要用于数字签名与密钥共享。杂凑算法主要用于数据完整性检验与消息认证。从算法和标准的角度来看,随着计算系统对数据安全的要求越来越高,密码算法和标准也不断更新。目前已成为标准的对称密码算法至少有 AES、3DES、Camellia 等数十种;

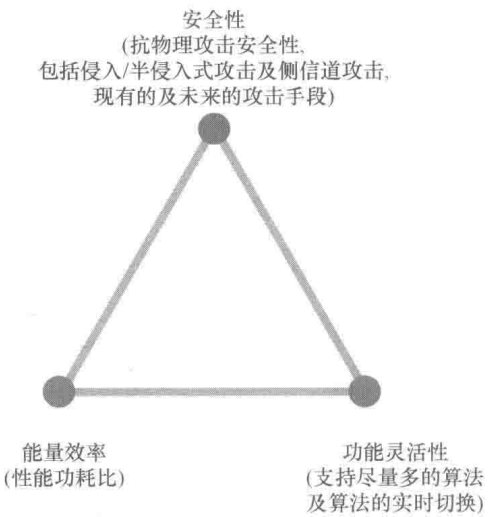


图 1.2.1 密码处理器应用需求

公钥密码算法有基于大数分解(如 RSA)、基于椭圆曲线离散对数(如 ECC)和基于数域上离散对数(如 ElGamal)的三大类;杂凑算法也至少有 MD5、SHA-2、SHA-3 等十余种。此外,每种算法又有很多变形。例如,对称密码 AES 根据密钥长度可分为 AES-128、AES-192、AES-256;公钥密码中的椭圆曲线加密算法根据所选数域与具体曲线的不同又存在多种变化;杂凑算法 SHA-3 根据摘要长度可分为 SHA-3-224、SHA-3-256、SHA-3-384、SHA-3-512[1,4]。更有甚者,为适应各种应用中不同的安全需求,每种密码又有很多独立于算法的执行模式可供选择。例如,每种分组密码都可以在电码本(electronic code book,ECB)、密文分组链接(cipher block chaining,CBC)和计数器(counter,CTR)等至少 5 种模式下运行[4]。所有这些因素组合起来会形成一个非常巨大的密码算法空间。从应用和协议的角度来看,一个常用的信息安全解决方案用到的密码算法就可能有数百种之多。例如,IP 层安全协议 IPsec 允许的密码算法就至少有 15 种之多:对称密码有 AES、DES、3DES、Blowfish、CAST、IDEA、RC4 和 RC6 等,公钥密码有 Diffie-Hellman 和 EC-DH 等,杂凑算法有 MD5、SHA-1、SHA-2、SHA-3 和 SM3 等;传输层安全协议 SSL 所支持的密码算法也有 Fortezza、RC2-40 和 DSS 等十余种[5,6]。尤其需要注意的是,这些安全协议具体在不同场景下使用哪个密码算法,还很有可能会根据会话协商的结果发生变化。

以上讨论的仅仅只是已成为标准的密码算法,一般用于商用领域。实际上,军事国防、航空航天、能源电力等这些特殊部门对密码算法安全性的要求更高,近乎苛刻。这些特殊部门往往根据自己的需要设计特定的密码算法。例如,通过改变线性反馈移位寄存器(linear feedback shift register,LFSR)的级数和抽头位置就