安全处理器研究进展

赵剑锋[1,2], 史 岗[1]

[1] 中国科学院信息工程研究所 第五实验室, 北京 中国 100093

[2] 中国科学院大学, 北京 中国 100049

摘要 信息安全已经影响到一个国家的政治、军事、经济和文化等诸多领域。信息一般在计算机系统上存储和处理。计算机系统的核心器件是处理器, 所以处理器的安全是计算机系统安全的基础, 也是信息安全的基础。在可信计算、工业控制、身份识别、网络通信、电子支付等许多行业, 都要用到安全处理器。文章对安全处理器发展过程进行了梳理, 并根据应用场景、功能进行了分类, 结合具体安全处理器架构, 分析了各主要安全处理器的技术特点和不足之处, 找出安全处理器研究中的规律。最后, 总结全文, 对安全处理器的研究进行了展望。

关键词 安全处理器; 分类; 特点; 展望
中图法分类号 TP309.2 DOI 号 10.19363/j.cnki.cn10-1380/tn.2018.01.009

Research Progress on Security Processor

ZHAO Jianfeng[1,2], SHI Gang[1]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

[2]University of Chinese Academy of Science, Beijing 100049, China

Abstract Information Security has influenced political, military, economic, cultural and many other fields of a country. Information is generally stored and processed in computer system. The core component of a computer system is CPU (central processing unit). Therefore, CPU security is the basis of both computer system security and information security. Security processors are used in such industries as trusted computing, industrial control, identity recognition, network communication and e-payment. After summarizing the security processor development process, this paper classifies key processors according to application scenarios. Combining the specific function and security processor architecture, it analyzes the features and shortcomings of main security processor technology and finds out the rules in security processor research. Finally, it offers research direction to the security processor.

Key words Security Processor; Classification; Feature; Prospect

1 引言

随着计算机技术的发展, 人们享受着信息交流的便利, 网上交易的快捷, 电子支付的简单。然而, 在这些信息处理的过程中, 涉及许多重要的数据, 如银行账户、密码、隐私文件及个人信息等。这些信息都需要在计算机或手持设备中存储、加工处理, 然而来自己软件、系统、芯片等诸多方面恶意攻击的威胁, 导致信息安全难以得到保障[1-8]。

信息安全已经影响到一个国家的政治、军事、经济和文化等许多领域, 影响着人们日常生活的方方面面。信息安全问题已成为国家信息产业发展的一个瓶颈。众所周知, 计算机系统是信息存储和处理的重要工具, 而处理器是整个计算机系统或手持设备的核心。处理器的安全是系统安全的基础。伴随着攻击技术的不断更新, 信息安全的防护也逐渐从软件向硬件过渡和转移, 如在可信计算、工业控制、身份识别、加密通信、电子支付等许多领域, 都要用到安全处理器[9-15]。

针对处理器的攻击方式主要包括物理攻击、逻辑攻击和应用攻击三种。

物理攻击方法包括计时攻击、故障攻击、能量

通讯作者: 赵剑锋, 博士研究生, 讲师, Email: zhaojianfeng@iie.ac.cn。
本课题得到国家“核高基”科技重大专项基金项目(No.2013ZX01029003-001); 国家“八六三”高技术研究发展计划基金项目(No. 2012AA01A401)资助。
收稿日期: 2016-09-19; 修改日期: 2016-11-15; 定稿日期: 2017-12-03

分析攻击、电磁波攻击、信息残留、穷举攻击、反向工程、微探测技术、FIB(Focused Ion beam)攻击、紫外线攻击、背面成像技术、主动光探测技术、热注入技术、冷冻探测。

例如, 早在 1998 年, 研究者 Markus G. Kuhn 针对一块具有总线加密功能的安全微控制器芯片进行了简单的修改, 使其可以利用个人电脑对微控制器与外部存储器之间的总线进行监听和篡改。随后通过观察总线状态与微控制器行为之间的关联, 成功地分析出了安全微控制器芯片的安全加密方式, 并获取了微控制器芯片在安全存储空间中经过加密处理的数据明文。

逻辑攻击分为缓冲区溢出、木马和病毒攻击、恶意程序攻击、未授权程序装载。

应用攻击分为密码体系攻击、软件漏洞攻击、固件攻击等。

由于存在上述诸多威胁, 对安全处理器的研究变得十分重要, 也十分必要。

有关安全处理器的综述主要有以下文献。

就国外而言, 2002 年, 文献[16]在对网络安全处理器研究的基础上, 提出了一种新的 IPSec 设计方案。随后, 2003 年, Esam Khan 等人对网络安全处理器的工作模式进行了总结, 分成三种, 即旁路模式、直通模式和集成安全模块模式[17]。

2006 年, R.Anderson 等人总结了密码处理器的详细应用, 以及密码处理器遇到的威胁和攻击: 入侵攻击(利用电子设备直接对处理器进行分析, 但是会破坏芯片), 半入侵攻击(对芯片进行分析, 但不破坏), 非入侵攻击(如功耗分析)及远程攻击(分析时序、协议、应用程序接口)。另外提出了相应的安全防范措施(如第三方认证、形式化验证等)[18]。

2009 年, R. Kannavara 和 N. G. Bourbakis 在综述文章中论述了安全处理器模型; 并根据加密引擎与处理器的位置关系分为: 加密引擎在处理器上, 加密引擎与处理器分离, 以及协处理器结构, 混合结构; 并对一些安全处理器进行了量化总结, 指出了安全处理器需要在安全性, 效率, 复杂性, 以及灵活性之间寻找平衡[10]。

2012 年, 文献[19]主要分析了对嵌入式处理器的攻击: 硬件攻击(如冷启动攻击、DMA 火线攻击、总线攻击)和软件攻击(如缓冲区溢出攻击、代码注入攻击)。另外, 总结了相应的安全措施(如看门狗检测、完整树、存储器加密), 并对各种方法进行了相应的对比研究。

2015 年, 文献[20]主要总结了各种加密算法, 如 AES、DES、RSA 在多核处理器上的应用, 并对多核处理器上各种加密算法的性能进行了分析。

就国内而言, 2007 年, 江南技术研究所的仲海梅和纪斌主要从以下几个方面进行了总结: 安全处理器以功能 IP 为基础的系统固件和电路综合技术结合, 处理器技术与安全技术为一体; 安全处理器的设计包括软件与硬件的划分、协同设计、协同仿真、电路综合和布局布线等; 安全处理器的特征; 安全处理器的应用等[11]。

2010 年, 华中科技大学的霍文捷在博士论文中对 2000 年到 2009 年之间的典型安全处理器架构进行了总结, 并分析了各个架构的特点[12]。

2011 年, 李超等人从安全处理器与网络处理器之间相互位置进行分类: 外置型、内置型和集成型, 并分析了它们的优点和缺点; 讨论了安全处理器的体系结构[13]。

2014 年, 清华大学的牛赟在博士论文中对网络安全处理器进行了综述。讨论了网络安全处理器的架构, 工业界现状, 学术界现状, 并对网络安全处理器的研究趋势进行了展望[21]。

2015 年, 华北电力大学的杨帆在论文中对安全处理器的规范问题进行了讨论; 研究了安全处理器相关文献; 安全处理器采用的核心技术[14]等。

与以上综述文献相比, 本文的贡献在于: 首次对通用处理器的架构研究进展做了总结, 找出研究规律, 并对关键的架构技术特点进行了分析; 按照处理器的应用场景进行了重新分类: 通用安全处理器, 网络安全处理器, 嵌入式安全处理器以及其他类安全处理器; 对于通用安全处理器, 网络安全处理器, 嵌入式安全处理器及其他类安全处理器, 通过列举典型案例, 揭示了安全处理器的演化过程; 最后, 在展望部分提出了明确的研究课题, 对推动国内安全处理器研究具有积极意义。

本文对安全处理器研究进展情况进行了总结; 对比了普通处理器与安全处理器的定义; 对安全处理器进行了分类, 在每一类中, 给出典型的安全处理器案例, 分析了每类处理器的技术特点和不足之处; 最后, 总结全文, 并对安全处理器将来的研究做了分析与展望。

2 安全处理器定义和分类

安全处理器与一般处理器不同。

一般处理器是指可以执行计算和控制程序的逻辑芯片, 主要包括控制单元、运算单元、存储单元和时钟。运算单元是计算机对数据进行加工处理的部

件, 由算术逻辑部件、寄存器组和状态寄存器组成。控制单元一般包括指令控制逻辑、时序控制逻辑、总线控制逻辑和中断控制逻辑等几部分。存储单元主要是指处理器内的指令缓存器和数据缓存器。

安全处理器除了具有一般处理器的功能和组成以外, 还要能够防止物理攻击、逻辑攻击或应用攻击。

按照安全处理器的应用场景可以分成四类: 通用安全处理器、网络安全处理器、嵌入式安全处理器和其他类。下一小节通过列举各类安全处理器的典型案例来揭示每类安全处理器的演化过程和特点。

3 各类安全处理器举例及特点分析

3.1 通用安全处理器举例及特点分析

3.1.1 单处理器架构

在通用安全处理器中, 比较典型的是斯坦福大学的 XOM 安全处理器架构, 以 XOM 架构为研究基础, 后续研究人员做了诸多改进。

下面结合典型案例, 对这个系列安全处理器架构的研究进展做详细的介绍。

2000 年, 文献[15]总结了内存受到的威胁, 比如欺骗攻击(spoofing attack), 重组、拼接攻击(splicing attack), 重放、重演攻击(replay attack), 相应地介绍了目前内存保护方面所采用的技术, 如斯坦福大学提出的 XOM(eXecute Only Memory)架构, 它用来保护数字版权问题。

XOM 在处理器内部有加密引擎, 程序运行在相互独立的存储隔间内(Compartment), 不同的数据属于不同的隔间, 系统运行时不允许程序访问其他隔间的数据[54]。下图是 XOM 架构示意图。XOM 上的软件由软件厂商进行加密, 它只能运行在特定的处理器上。为了增加安全性并且提高性能, 根据对称加密算法(处理速度相对快)和非对称加密算法(处理速度相对慢)在性能上的不同, XOM 使用了密钥共享协议。首先, XOM 处理器芯片中存储一对非对称密钥对(Kxom, Kp), 其中, Kxom 为私钥, Kp 为对外公开的公钥。应用程序发布者使用自己的对称密钥 Ks 对程序加密生成相应的密文, 然后通过用户处理器公钥 Kp 来加密密钥 Ks, 最后将程序密文和加密后的 Ks 一起发给用户。系统运行此应用软件时, 先使用自己的私钥 Kxom 来解密得到软件密钥 Ks, 然后通过 Ks 来解密程序并运行。通过这种方法, 软件发布者可以通过使用相应的处理器公钥 Kp 来加密 Ks, 从而使得相应的程序只能运行在特定的处理器上, 实现了对软件版权的保护。

另外, XOM 还通过为流出处理器的数据附加

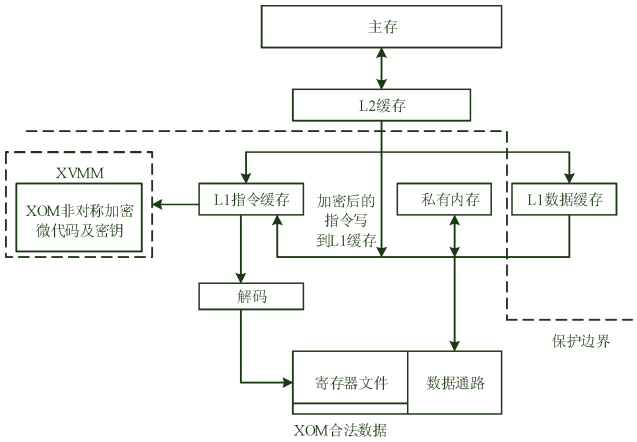

图 1 XOM 安全模型示意图

Figure 1 Schematic diagram of the XOM security model

MAC 值来实施完整性保护。通过将地址合并计算在 MAC 中, XOM 可以阻止攻击者替换不同地址处的存储器块来破坏完整性。不过, XOM 无法对抗重放攻击。

2003 年, 麻省理工学院人工智能实验室的 B.Grassend 等人在 XOM 架构的基础上提出 CHTree (Caches and Hash Trees) [23],它利用了 Merkle 树的方法对存储器中的程序或数据进行完整性验证。但是, 这种方法对系统性能影响较大, 导致性能最少下降 25%。另外, 文献[31, 34, 37, 49]主要对 CHTree 方法进行了研究和不同的改进。

加州大学的 J.Yang 等研究人员研究了 XOM 的硬件实现, 并进行了改进, 提出了 OTP(One-Time-Pad)方法来保护外存数据的机密性。该方法优点是提升加解密速度, 在原 XOM 基础上,性能最大提升 34.7%, 缺点是增加了存储开销[28, 29]。文献[32, 48]对 OTP 方式进行了研究和改进。

2003 年, 该实验室的 G.E. Suh 等人结合 OTP[29] 加密方式及 CHTree[23]校验方式提出了 AEGIS (Architecture for Tamper-Evident and Tamper-Resistant Processing)架构, 它对内存的数据提供了机密性和完整性保护[24]。它假定处理器和操作系统的部分内核是安全的(Security Kernel)。它提供了两种工作模式: TE(Tamper-Evident)和 PTR(Private and authenticated Tamper-Resistant)。TE 为系统数据提供了完整性保护, 确保软件运行过程中能够探测到对数据的篡改行为。PTR 提供了对数据的完整性和机密性保护。AEGIS 架构如下图 2 所示。

在 Security Kernel 中, AEGIS 采用安全上下文管理器 SCM(Secure Context Manager)来维护每一个进程的相关安全信息。每条记录如下表所示。

其中, SPID 为安全进程 ID, 值为 0 时表示不受安

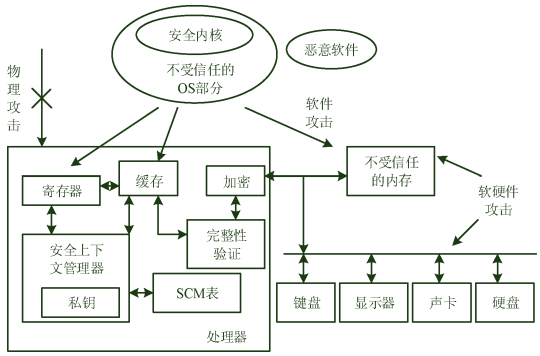

图 2　AEGIS 安全模型示意图

Figure 2　Schematic diagram of the AEGIS security model

表 1　AEGIS 的进程安全条目[24]

Table 1　AEGIS's process security entry [24]

SPID	H(Prog)	Regs	Hmem	0/1	Kstatic,Kdynamic

全保护的普通进程。H(Prog)表示相应的哈希值。Regs 代表相应的寄存器及其值。Hmem 用于完整性校验。0/1 表示该进程的工作保护模式状态(TE 或 PTR)。Kstatic 为对称密钥, 用于加解密应用程序, 每个应用程序都有一个唯一的 Kstatic, 在程序运行过程中保持不变。程序运行过程中产生的数据使用 Kdynamic 进行加密, 不同会话产生的 Kdynamic 是不同的, 在会话结束时该密钥也就失效了。

AEGIS 架构不仅可以用于软件版权保护, 也可以用于认证执行和数字版权管理上, 但就机密性和完整性而言, AEGIS 采用了直接块加密和 Hash 树校验方法, 系统延迟开销较大, 效率较低, 实用性不是很强。

Cerium[74]是 MIT(麻省理工学院)提出的另外一种可信处理器。它结合了 XOM 和 AEGIS 处理器优点, 通过加密被保护进程的地址空间来实现类似 IBM4758 中的认证执行。它不是采用硬件加密, 而是采用软件方式来加密保护进程。它将一个可信微内核放入处理器内部, 对被保护进程地址空间的所有

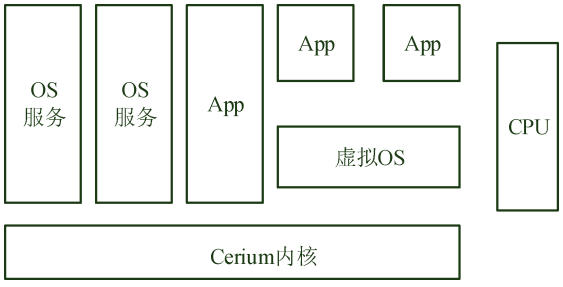

图 3　Cerium 系统结构示意图

Figure 3　Schematic diagram of Cerium system structure

操作都会触发这段微内核代码, 由它来处理加密地址空间。

2006 年, C.Y. Yan 等人在 AES-GSM(AES-Galois/Counter Mode)基础上, 对完整性检验方法做了改进, 它采用了分段式计数器来实现时间戳[35]。AES-GSM[36]算法将数据的加解密和完整性验证的时间延迟隐藏在系统访存的过程中, 处理器在做完整性校验时获得了较好的性能, 这种性能的提升主要依靠 AES-GSM 算法。但是作者依然采用完整树校验方法, 所以影响性能的提升。

2006 年, R. Elbaz 等人提出了 PE-ICE 的加密认证方式[38]。PE-ICE 基于数据块加密, 它的优点在于做加密运算的同时, 进行完整性计算, 从而大大提高处理器性能。它的缺点是完整性标签保存在片外存储器, 同样有安全隐患。2007 年, R. Elbza 等在 PC-ICE 的基础上提出了 TEC-Tree 方法[43]。TEC-Tree 将节点认证与完整树更新过程并行处理, 提升了处理器性能。但是它只是一个理论模型, 没有硬件实现和相应的性能评估。文献[63]对 PE-ICE 架构进行了研究和改进。

2007 年, W.D. Shi 等人对存储器加解密方式作了进一步改进, 提出基于使用频率的密文预测机制来提升解密的性能[41]。基本原理是: 在处理器内设计一组频率表, 用来记录相应的数据值的使用频率, 并对使用频率高的密文进行快速缓存, 通过这种方式可以得到 10%至 20%的性能加速比, 不过这种方法是以增加硬件开销为代价的。

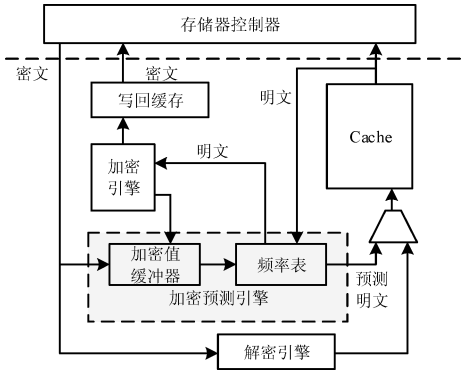

图 4　频率预测表加密机制示意图

Figure 4　Schematic diagram of frequency prediction table encryption mechanism

2007 年, B. Rogers 等人提出了 BMT(Bonsai Merkle Tree)完整性校验方法[42], 设计了一种与地址无关的加密方法。BMT 并不对全部数据块进行加密, BMT 只对加密用到的计数值进行完整性校验, 它不使用完整树, 需要消耗额外的存储空间, MAC 值保存在片外, 安全程度不高。

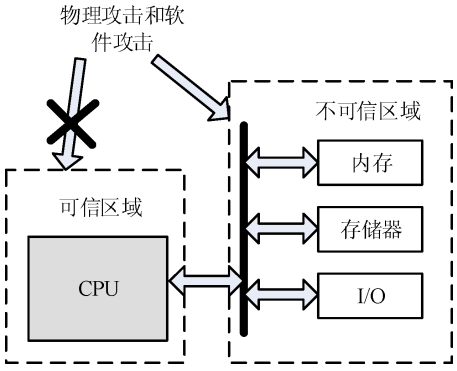

图 5 安全模型示意图

Figure 5 Schematic diagram of security model

以上所述的安全处理器的假设攻击模型如下图所示, 在该模型中, 认为存储器和 I/O 设备硬件部分容易受到攻击。为了保护存储器数据的机密性和完整性, 在处理器中加入了相应的密码运算和完整性运算等模块。

现把与 XOM 架构相关的安全处理器的特点列在表 2 中。

3.1.2 多处理器架构

2004 年, 乔治亚理工学院的 W.D. Shi 等研究人员提出了多处理器安全架构来保护外存数据的机密性和完整性[23]。其架构原理图如下所示。

表 2 以 XOM 架构为基础的安全处理器特点分析

Table 2 Analysis of the characteristics of security processor based on XOM architecture

年代	名称	机密性	完整性	特点	性能
2000	XOM[15]	有 (对称加密和公钥加密)	有	防止对外存的欺骗攻击和重组攻击	性能下降小于 50%
2003	CHTree[23]	有 (对称加密和公钥加密)	有 (Merkle 树)	在 XOM 基础上提供完整性保护	性能下降至少为 25%
2003	OTP[29]	有 (OTP 加密方法)	有	在 XOM 基础上加快加解密速度, 但是增加存储开销	提升性能 34.7%
2003	AEGIS[24]	有 (OTP 加密方式)	有 (CHTree 完整性校验)	结合 OPT 与 CHTree 方式, 提供 TE 与 PTR 两种方式	TE 模式性能下降小于 20%, PTR 模式性能下降大于 50%
2003	Cerium[74]	有	有	结合 XOM 和 AEGIS 优点	未给出
2005	LHash[31]	有	有	对 CHTree 进行改进	性能下降不超过 16%
2005	预测加密[32]	有	有	在 OTP 基础上改进	提升性能 15%到 40%
2005	热窗口 Merkle 树优化[34]	有	有	对 Merkle 树进行优化	性能损失一般在 15%, 最大为 35%
2006	基于 AES-GSM 时间戳[35]	有	有	采用分段式计数	提升性能 20%
2006	M-tree[37]	有	有(SHA-256)	对 CHTree 改进	性能提升至少 10%
2006	PE-ICE[38]	有	有	加密与完整性同时进行	和块加密方式相比, 提升 4%
2007	基于频率预测加密[41]	有	有	基于使用频率	提升性能 10%到 20%
2007	BMT[42]	有	有	对部分值进行校验	提升性能 2%到 12%
2007	TEC-Tree[43]	有	有	对 PC-ICE 改进	理论模型, 没有硬件实现
2009	OTP+CRC[47]	有	有	结合 OTP 和 CRC 特点	提升性能 40%
2009	ShMAC[49]	有	有	提升 MAC 计算性能	无硬件评估
2012	PCIP[63]	有	有	对 PE-ICE 进行改进	提升性能 10%左右

2005 年, Y.T. Zhang 等人提出了 SENSS(Security Enhancement to Symmetric Shared Memory Multi-processor)架构[33], 该架构保护 SMP 下的缓存之间消息的安全传输及校验。每个处理器拥有自己的 L1 和 L2 缓存, 所有的处理器通过总线共享内存。其架构如图示。在 SENSS 架构中, 每个处理器有唯一的公钥对$(S_i,t_i)i=0,1, \ldots, n$。软件厂商利用对称加密钥 k 对程序进行加密, 然后使用处理器的公钥 S_i 对对称密钥进行加密, 然后将程序密文和加密后的密钥 k 分发给系统, 程序发布者可以指定特定的处理器来执行程序。图中显示了应用程序 1 使用处理器 0、1、2 来执行, 而应用程序 2 使用了处理器 2 到 n 来执行, n 表示处理器最大标识(PID)。特定的处理器分成一组(group), 每组有唯一的标识(GID)。

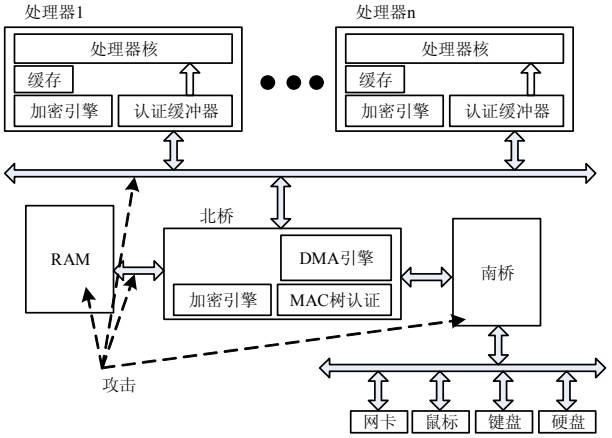

图 6 多处理器安全架构示意图

Figure 6 Multi processor security architecture schematic

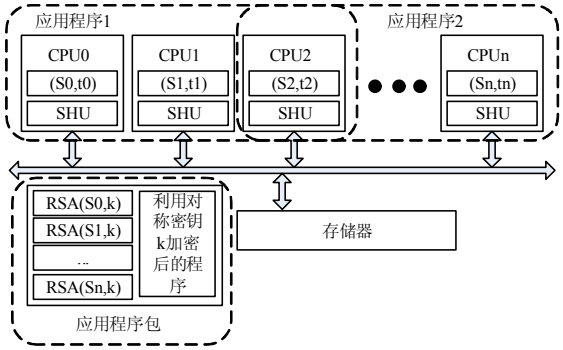

图 7 SENSS 结构示意图

Figure 7 Schematic diagram of SENSS structure

为了保护某组消息不被其他组篡改, SENSS 为每个处理器配置了一个安全硬件单元 SHU(security hardware unit), 该单元只能由硬件来控制, 软件层(应用程序和操作系统)无权访问。

多处理器的安全假设与单处理器类似, 也是认为存储器易于受到攻击, 为了保护存储器数据的机密性和完整性, 每个处理器架构与单处理器安全架构类似, 不过, 由于是多处理器架构, 又增加了其他一些硬件开销来管理或协调各个处理器之间的通信及数据传输。

3.2 网络安全处理器举例及特点分析

网络安全处理器是网络安全设备的基础核心器件, 它包括数据传输、安全协议处理和密码运算三个部分, 其框架图如下所示[21]。

网络安全处理器经历了三个发展阶段, 第一阶段主要是实现密码算法运算及认证或密钥交换算法, 第一阶段采用的网络安全处理器架构主要是通用处理器与 ASIC 相结合, ASIC 实现密码运算和协议处理; 第二阶段集成了安全协议处理和密码运算功能, 第

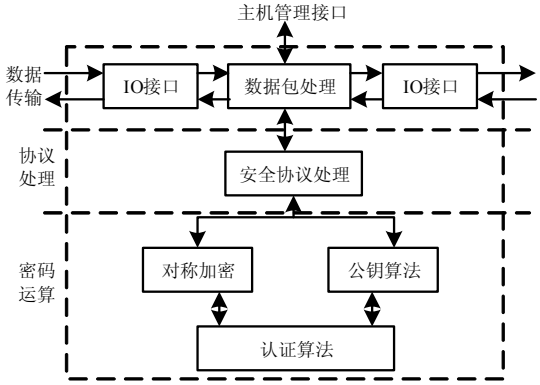

图 8 网络安全处理器功能框架图

Figure 8 Network security processor functional framework diagram

二阶段采用网络处理器与安全模块相结合的结构, 网络处理器完成协议处理, 路由查找, 数据包调度功能, 安全模块负责相应的安全功能; 第三阶段集成了高速数据传输模块, 网络安全处理器位于数据通路上, 这个阶段网络安全处理器采用 SoC 结构, 由数据传输模块、安全协议处理和密码运算三部分组成[21]。

比较典型的案例如下所述。

2002 年, M. McLoone 和 J.V.McCanny 提出了基于 IPsec 的加密处理器[16]。如下图所示, 该处理器中加入了 Rijindael 加密算法逻辑电路, 以及 HMAC-SHA-1 认证算法逻辑电路。

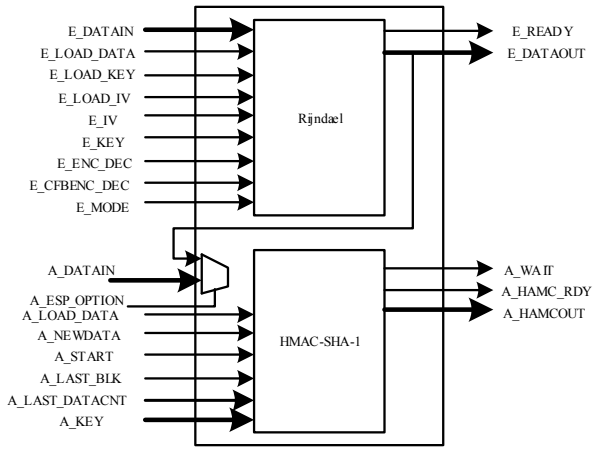

图 9 IPSec 加密核示意图

Figure 9 IPSec encrypted kernel schematic

就国内网络安全处理器研究而言, 处理器架构基本上也是基于 IPsec, 主要是在这种架构基础上, 通过增加安全协议、提高传输速率等手段来提高网络安全处理器的安全性和整体性能[25, 39, 70, 73]。典型案例如下所述。

例如, 2010 年, 清华大学微电子学研究所的王海欣等人设计了高性能网络安全处理器[56]。该处理器支持 IPsec、SSL/TLS 网络安全协议, 采用系统级流水线和双路单向总线设计, 提高数据通路的传输速率, 缓解了总线仲裁和数据拥塞。

2014 年, 文献[21]研究并实现了单通道 10Gbps 在线网络安全处理器。它在分析 IPsec 协议基础上, 采取基于流水线的交叉开关总线数据传输通路, 实现多模块之间数据的同时传输。另外, 提出了一种密码算法片外可扩展机制, 通过嵌入式 CPU 配置即可实现外片专用算法替换片内通用算法的功能。

网络安全处理器结构相对来说比较单一, 现在主要采用 SoC 结构来实现, 数据传输采用 DMA 方式, IPSec 协议一般由 SoC 内部的 CPU 来完成, 另外, 有关密码运算的功能由单独的硬件模块来实现[21]。

3.3 嵌入式安全处理器举例及特点分析

嵌入式安全处理器的架构借鉴了通用安全处理器架构的一些方法, 来保护数据的机密性和完整性[13, 61], 但也有不同之处。

比较典型的案例如下所述。

第一, TrustZone 是 ARM 针对消费电子设备安全提出的一种安全系统架构[51]

就处理器架构而言, 每个物理的处理器核提供两个虚拟核, 一个非安全核(Non-secure, NS)和一个安全核(secure), 非安全核与安全核之间的切换机制叫做 monitor 模式。非安全核只能访问普通世界的系统资源, 而安全核能访问所有资源。普通世界的软件想进入到 monitor 模式, 可以使用 SMC 指令或者通过硬件异常机制的一个子集实现。可以配置 IRQ, FIQ, 外部 data abort, 外部 prefetch abort 这几个异常进入到 monitor 模式。下图展示了这种切换方式。

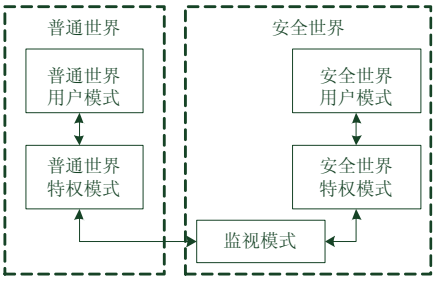

图 10 TrustZone 切换示意图

Figure 10 TrustZone switching schematic diagram

一般情况下, 如果普通世界的用户模式需要获取安全世界的服务时, 它要先进入到普通世界的特权模式, 在该模式下调用 SMC, 那么处理器进入到 monitor 模式, monitor 模式备份保存普通世界的上下文, 随后进入到安全世界的特权模式, 此时的运行环境变成了安全世界的执行环境, 然后再进入到安全世界的用户模式, 执行相应的安全服务。这里把安全世界的用户模式和特权模式分离, 是因为通过特权模式中的执行环境是系统级别的, 而用户模式的安全服务是应用级别的, 两者的提供者通常是不同的。下图是软件架构的展示。安全世界的执行环境要管理用户模式的服务和应用, 并给它们提供编程接口。

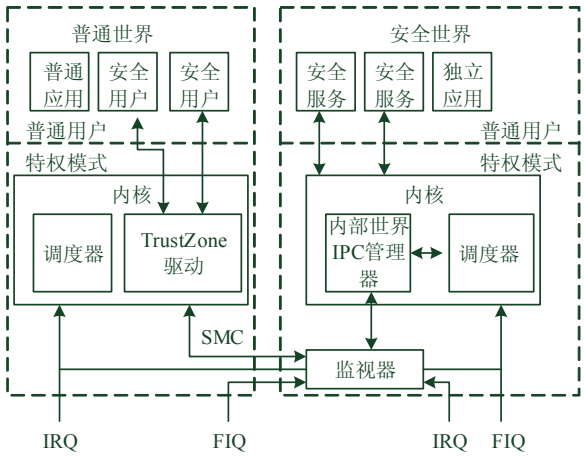

图 11 TrustZone 软件架构示意图

Figure 11 Schematic diagram of TrustZone software architecture

第二, 2009 年, A. Rogers 等人提出了一种嵌入式安全处理器架构[52]。该架构包括三个阶段: 安全程序安装, 安全载入和安全执行。在安全安装阶段, 利用验证架构, 对可执行二进制程序进行修改, 产生一个安全的可执行文件。安全载入为安全运行做准备。在安全运行阶段, 对执行的程序进行运行检验来保证完整性和机密性。这个架构可以提供以下几种模式: 程序无保护执行模式, CIOM(Code Integrity Only Mode), CICM(Code Integrity and Confidentiality Mode), DIOM(Data Integrity Only Mode), DICM(Data Integrity and Confidentiality Mode),以及这几种模式的组合。

第三, 防止侧信道攻击和恶意硬件电路的设计[59, 65]。

例如, 2014 年, 文献[66]提出了一种安全的不可克隆的嵌入式处理器设计。该处理器安全的前提是: 机器码与执行环境之间要使用内置在处理器中的 PUFs 进行相互验证。在该系统中, 指令在内存中有两种形式 obfuscated 和 challenge word, obfuscated 指令不能被处理器执行, 要想被执行, 需要把 challenge word 发送到 PUF, 根据 PUF 的响应(Response)再结合 obfuscated 指令恢复出正确的操作码, 然后才可以执行。

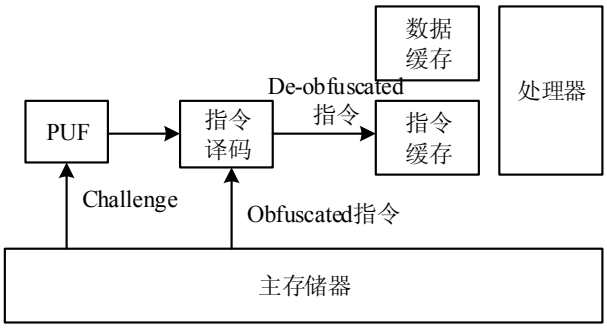

图 12 不可克隆嵌入式处理器结构图[62]
Figure 12 Non-cloned embedded processor structure diagram [66]

3.4 其他安全处理器举例及特点分析

第一种, 保护数据机密性和完整性, 防止侧信道攻击及功耗分析。比较典型的是在处理中加入各种加密算法模块, 如椭圆曲线加密模块, RSA 加密模块[26, 30, 40, 44-46, 54, 57, 60, 67-69]。

例如, 2015 年, 文献[68]提出了一种防止侧信道攻击的安全处理器架构。它的原理是: 通过随机调度器对每条指令的执行做随机延迟, 从而使每条指令的执行功耗随机化, 增加侧信道功耗分析攻击的难度。

第二种, 防止缓冲区溢出攻击。例如, 2003 年, 普林斯顿大学的 J.P. McGregor 等人提出了一种针对缓冲区溢出攻击的处理器架构[22]。该处理器中增加了一个安全返回地址栈, 它可以提供内置的、动态的保护, 防止对返回地址进行攻击, 而且不需要用户和应用程序的干预, 对性能几乎不产生影响。

第三种, 防止硬件木马攻击。2009 年, 文献[50]提出: 在芯片中加入监测和防御模块, 包括传感器、中央控制逻辑和信号控制单元等, 如下图所示。其中信号探测(signal probe networks, SPN)模块是可编程的, 实现了对正常电路信号进行选择采样监测; 安全监视(security monitors, SM)模块也是可编程的, 它负责分析 SPN 送来的信号; 安全控制和处理模块实现对 SPN 和 SM 模块的重配置编程, 而配置数据则以加密的方式存放在安全FLASH中; 加密/解密模块对存放在安全 FLASH 中的数据进行加密和解密; 一旦监测模块发现异常, 信号控制模块能提供相应的应对措施, 以防止危险的发生。

第四种, 让程序安全执行[53, 55, 58, 62, 64, 68, 71-72]。

例如, 2013 年, 文献[64]提出了一种检测 CPU 操作码的保护单元, 即 PPU(processor protection unit)。如下图所示。PPU 检查操作码的合法性、操作码执行时钟周期的合法性、有限状态机的合法性及处理器内部信号的合法性。通过检验操作码的取值, 可以

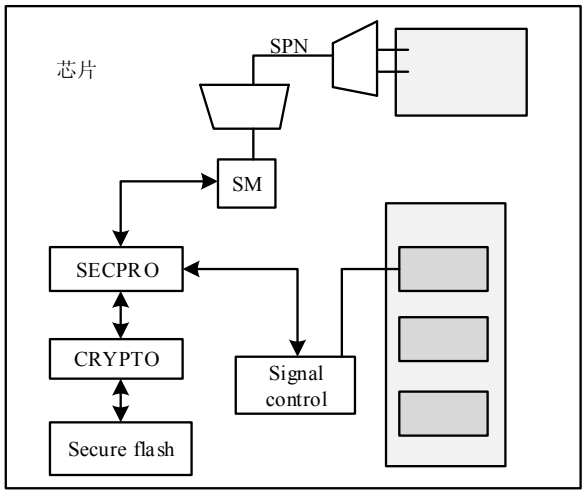

图 13 包含信号探测与监视模块的芯片架构
Figure 13 Chip architecture with signal detection and monitoring modules

防止攻击者在处理器中植入恶意的指令。有限状态机的验证可以防止攻击者执行非法行为的企图。

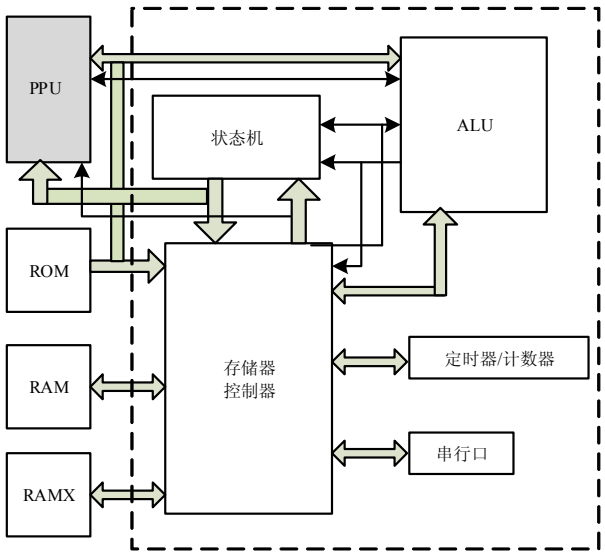

图 14 PPU 保护示意图
Figure 14 Schematic diagram of PPU protection

还有, 文献[72]提出了一种基于乱码电路的 GarbledCPU 架构, 可以支持高级语言函数的安全运行。其架构示意图如下, Alice 产生乱码指令(Garbled instruction) 和乱码表(Garbled table), 通过 OT (Oblivious Transfer)发给 Bob, Bob 通过 GarbledCPU, 估算出乱码输出, Alice 提供输出映射(Output Map), Bob 最终恢复出原始数据。

4 总结与展望

通过对安全处理器进行分类、举例, 以及特点分

析, 可以总结出以下几点结论。

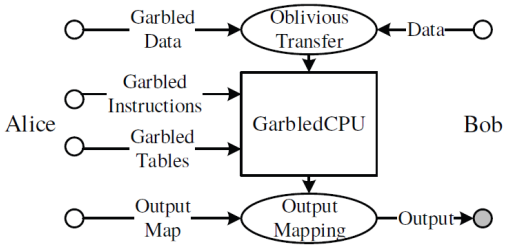

图 15 GarbledCPU 示意图[68]

Figure 15 GarbledCPU schematic diagram[68]

(1) 通用安全处理器的研究前提是假设外部存储器易于受到攻击, 为了保护外部存储器数据的机密性、完整性, 从而在处理器中加入了相应的密码运算和完整性校验模块。但是, 一旦加入加解密运算和完整性运算之后, 必然会导致系统性能下降, 所以, 整个研究主线是围绕如何在保证外部存储器数据机密性、完整性的同时, 尽可能地降低对系统性能的影响。通用安全处理器中涉及的密码算法主要有对称加密算法 DES、AES, 以及非对称加密算法 RSA、ECC 等; 涉及的完整性校验算法主要有 Merkle 树完整性校验, 以及对 Merkle 树改进的完整性校验算法。研究的难点在于如何在保证外部存储器数据机密性、完整性的同时, 花费尽量小的性能代价和硬件代价。另外, 有关多处理器安全架构, 其基本假设与单处理器类似, 也是为了保护存储器数据的安全性, 只不过处理器的个数增加, 从而使架构变得更为复杂, 需要加入额外的硬件开销来实现。

(2) 通过对网络安全处理器的研究发现, 在网络安全处理器中, 实现网络安全协议规范中有关密码运算的部分一般采用硬件来实现; 对于网络安全协议的实现而言, 可以在软件层面(通用软件或操作系统)实现, 也可以用通用硬件来完成。网络安全处理器的研究主要着眼于高性能密码算法模块的实现, 以及优化硬件结构, 提高数据的吞吐率, 减小芯片面积。最近几年, 基于 IPSec 的安全处理器主要集中在如何降低功耗、采用多核处理器及结构可扩展的研究上。

(3) 嵌入式设备, 尤其是以手机为代表的手持嵌入式设备与人们的生活密切相关, 在这些嵌入式设备中存储着重要、敏感的数据信息, 如账户、密码等。但是, 由于嵌入式设备易于获取, 加上应用环境复杂, 致使恶意攻击者可以绕过软件安全机制对嵌入式系统展开攻击。事实上, 很多安全漏洞来自嵌入式底层硬件设计的不合理性以及疏漏, 如果攻击者获取了嵌入式设备, 则可以采用多种方式来获取嵌入式设备上的有价值的信息。关于嵌入式安全处理器的研究, 一般先分析嵌入式处理器运行过程中面临的潜在威胁, 根据威胁来针对性地提出嵌入式安全处理器架构, 同时要在成本、性能、功耗以及面积等因素之间进行权衡。

(4) 有关其他类安全处理器, 基本上是与上述三类是相关的或相近的, 只不过为了解决特定问题而设计的, 如有的为了防止缓冲区溢出[22], 有的为了防止侧信道攻击[69, 71]等。但是, 如果涉及数据机密性和完整性保护, 则与其他三类安全处理器类似, 基本上要采用对称加密算法、流密码算法及非对称加密算法等。这也是所有安全处理器的共同点(保护数据机密性和完整性)。

目前我国的高端、高档处理器主要依赖进口,对于那些应用于国防系统、政府机构、金融、交通等安全敏感领域的处理器来说, 供应过程的不可控, 使得在使用这些芯片时面临极大的安全隐患: 攻击者可以在设计或制造过程中往芯片中植入恶意硬件, 这些恶意可能在将来某个时候被攻击者触发, 也可能在某些情况下自行触发。因此, 处理器的自主可控是信息安全的基石和保证。虽然我国在安全处理器上已经展开了研究, 但刚刚起步, 还有很多工作要做。对于我们来说, 有如下几个问题值得研究。

(1) 有关通用安全处理器的研究目前主要集中在对外部存储器数据机密性和完整性保护上, 研究范围相对较窄。虽然有少数针对缓冲区溢出攻击、侧信道攻击的安全处理器, 但是研究尚未形成热点。因此, 下一步的工作, 应该在结合目前通用安全处理器架构优点的基础上, 进一步优化性能, 在控制安全处理器功耗水平和芯片面积的基础上, 逐渐增加更多、更难的功能, 另外, 要考虑加解密速度、灵活性及可配置性等性能。

(2) 关于网络安全处理器, 主要研究方向为异质多核、计算密集型的 SoC 数据流处理的研究, 例如, 如何提高核的使用效率, 降低核的数量, 另外, 提高数据传输效率也是难点和挑战; 异质多核 SoC 的设计验证问题也是值得研究的, 因为增加核的数量以后, 测试周期和测试向量都会急剧增加, 如何降低测试成本, 提高验证效率, 这些都是新的研究课题。再者, 在网络通信中要考虑到侧信道信息泄漏的问题, 对抗侧信道攻击方法的研究是非常重要的, 也是十分必要的[21]。

(3) 嵌入式处理器在军事、金融、通信、交通等许多安全敏感领域应用广泛, 所以对嵌入式安全处理器展开研究也是十分重要的。由于嵌入式处理器

是针对某一特殊领域的需求设计的, 所以设计方要按照应用环境的需求来对芯片做出规划, 要保证成本最低、性能最优。由此, 在嵌入式安全处理器研究中, 要考虑到加解密运算的延迟开销, 带宽开销, 以及密钥管理带来的存储开销。与此同时, 功耗也是嵌入式系统的一项重要的性能指标, 在考虑安全的同时, 要考虑功耗开销问题, 也就是说, 在设计嵌入式安全处理器时, 要把成本、性能、功耗和安全性全面客观地权衡, 只有这样, 才有可能设计出实用的嵌入式安全处理器[13]。

致谢 本文是在对安全处理器的调研基础上完成的, 通过对有安全处理器的文献资料研究分析, 跟踪安全处理器研究进展情况。本文是在信息工程研究所第五研究室多位老师指导下完成的, 在此表示诚挚感谢。另外, 对于审稿专家的意见和建议, 表示衷心感谢!

参考文献

[1] P. Jiang, D.J. Li. “Information countermeasure”. *Tsinghua University press, Chinese People's Public Security University press*, pp.8-11. 2007(蒋平，李冬静. “信息对抗”.*清华大学出版社, 中国人民公安大学出版社* 2007:8-11.)

[2] B.Kauer, OSLO: Improving the security of Trusted Computing, *16th USENIX Security Symposium (Security'07)*, pp.229-237. 2007.

[3] J.Winter. Trusted Computing Building Blocks for Embedded Linux-based ARM Trust Zone Platforms, *Proceedings of the 3rd ACM workshop on Scalable trusted computing (STC'08)*, pp. 21-30.2008.

[4] IBM, Microsoft, etc.Workshop on Advancing Computer Architecture Research (ACAR-II): Laying a New Foundation for IT, *Computer Architecture for 2025 and beyond*, pp.1-20, 2010.

[5] McAfee Corp. New Paradigm Shift: Comprehensive Security beyond the Operating System. *White paper*, pp.1-10, 2012.

[6] A.Sanjaya, Hardware Assisted Security: Anticipating Digital Threat and Challenges. *FIRST TC 2012 IDF (TC'12)*, pp.1-10, 2012.

[7] Ruby B. Lee. Hardware-Enhanced Security. Keynote, *ACM CCS,* 2012.

[8] “EMET Technology”,https://windowssecrets.com/top-story/protecting-pcs-from-the-next-zero- day-threat/. Sept.2013.

[9] C. Shu, S.W. Li, W.J. Zhang and K.F. Feng. “Research of Networking Security Processor”. *Journal of the Graduate School of the Chinese Academy of Sciences*, vol.19, no.1, pp. 97-101, 2002. (舒昶, 吕述望, 张文清, 冯凯锋, 网络安全处理器的研究[J]. *中国科学院研究生院学报*, 2002, 19(1): 97-101)

[10] R. Kannavara and N. G. Bourbakis, “Surveying secure Processor”. *IEEE potentials*, vol.28, no.1, pp.28-34, 2009.

[11] H.M. Zhong and B. Ji, “Research of security processor”. Computer & Information Technology, no.5, pp. 70-72, 2007. (仲海梅, 纪斌, 安全处理器的研究[J] . *计算机与信息技术*, 2007，5：70-72)

[12] W.J. Huo. “Research and Design of Secure Run-time Mechnasim for Embedded Processor [Ph.D.dissertation]” , *HuaZhong University of Science and Technology*, 2010. (霍文捷. 嵌入式处理器安全运行机制的研究与设计[博士学位论文], *华中科技大学*, 2010.)

[13] C. Li, M.L. Zhang, X. Yang, Y.J. Xu and Z.Y. Luo, “Status and Prospects of Security Processor Architecture”. *Journal of Chinese Computer Systems*, vol.32, no.10, pp.1942-1946, 2011. (李超，张美琳, 杨旭, 徐勇军, 骆祖莹, 安全处理器体系结构的现状与展望[J] . 小型微型计算机系统, 2011, 32(10) : 1942-1946)

[14] F. Yang. “Research on Security Processor ”, *North China Electric Power University*, 2015. (杨帆. 安全处理器研究[硕士学位论文], *华北电力大学*，2015.)

[15] D. Lie, C. Thekkath, M. Mitchell, P. Lincoln, D. Boneh, J. Mitchell and M. Horowitz. Architectural Support for Copy and Tamper Resistant Software. *In Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating System (ASPLOSIX'2000)*, pp.169-177, 2000.

[16] M. Mcloone and J.V. McCanny. A single-chip IPSEC cryptographic processor. *Signal Processing Systems (SIPS'02)*, pp.133-138, 2002.

[17] E. Khan, M.W. El-Kharashi, A.N.M. Ehtesham Rafiq, F. Gebali and M. Abd-El-Barr. Network Processors for Communication Security : A Review. *2003 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing(PACRIM'03)*. pp. 173-176, 2003.

[18] R. Anderson, M. Bond, J. Clulow, and S. Skorobogatow. Cryptographic Processors-A Survey. *Proceedings of the IEEE*, vol. 94, no.2, pp.357-369, 2006.

[19] A.K. Kanuparthi, R. Karri, G. Ormazabal and S.K. Addepalli. A Sruvey of Microarchitecture Support for Embedded Processor Security. *2012 IEEE Computer Society Annual Symposium on VLSI(ISVLSI'12)*, pp.368-373, 2012.

[20] V. Jain, P. Sharma and S. Sharma. Cryptographic Algorithm on Multicore Processor : A Review. *2015 International Conference on Advances in Computer Engineering and Applicatons (ICACEA'15)*, pp.241-244, 2015.

[21] Y.Niu. “Research and Implementation on Single Channel 10Gbps In-Line Network Security Processor[Ph.D.dissertation]” , *Tsinghua University*, 2014.(牛赟. 单通道 10Gbps 在线网络安全

处理器设计研究与实现[博士学位论文], *清华大学*，2014.)

[22] J.P. McGregor, D.K. Karig, Z. Shi and R.B. Lee. A processor architecture defense against buffer overflow attacks. *Proceeding of Information Technology Research and Education(ITRE'03)*, pp.243-250, 2003.

[23] B. Grassend, G. E. Suh, D. Clarke, M.V. Dijk and S. Devadas. Caches and Hash Trees for Efficient Memory Integrity Verification. *The 9th International Symposium on High- Performance Computer Architecture(HPCA'03)*, pp.295-306, 2003.

[24] G.Suh, D.Clarke, B.Gassend, M.dijk and S.Devadas. AEGIS: Architecture for Tamper-Evident and Tamper-Resistant Processing. *In Proc. International Conference of Supercomputing (ICS'03)*, pp.160-171, 2003.

[25] Y. Zhang and Z.G. Sun. Research on the Architecture of the Nest Generation High-performance Network Security Processor Based on IPSec. *Journal of National University of Defense Technology*, no.2, pp.64-67, 2003. (张怡，孙志刚. 基于 IPSec 的下一代高性能安全处理器的体系结构. *国防科技大学学报[J]*. 2003, 2: 64-67.)

[26] H.Eberle, N. Gura, S.C. Shantz, V. Gupta and L. Rarick. A Public-key Cryptographic Processor for RSA and ECC. *Proceeding of the 15th IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP'04)*, pp.98-110, 2004.

[27] W.D. Shi, H.H.S. Lee, M. Ghosh and C.H. Lu. Architectural Support for High Speed Protection of Memory Integrity and Confidentiality in Multiprocessor Systems. *Proceedings of the 13th International Conference on Parallel Architecture and Compilation Techniques(PACT'04)*, pp.123-134, 2004.

[28] J. Yang, Y.T. Zhang and L. Gao. Fast Secure Processor for Inhibiting Software Privacy and Tampering. Proceedings of the 36th International Symposium on Micro architecture (MICRO'03), pp.351-360, 2003.

[29] J. Yang, L. Gao and Y.T. Zhang. Improving Memory Encryption Performance in Secure Processor. IEEE Transactions on Computer, vol.54, no.5, pp.630-640, 2005.

[30] R.B. Lee, P.C.S. Kwan, J.P. McGregor, J. Dwoskin and Z.H. Wang. Architecture for protecting Critical Secrets in Microprocessors. *Proceedings of the 32nd International Symposium on Computer Architecture (ISCA'05)*, pp.2-13, 2005.

[31] G.E. Suh. AEGIS: A single-chip secure processor. *Information Security Technical Report*, vol.10, no.2, pp.63-73, 2005.

[32] W.D. Shi, H.S. Lee, M. Ghosh, C.H. Lu and A. Boldyreva. High Efficiency Counter Mode Security Architecture Via Prediction and Precomputation. *Proceedings of the 32nd International Symposium on Computer Architecture (ISCA'05)*, pp.14-24, 2005.

[33] Y.T. Zhang, L. Gao, J. Yang, X.Y. Zhang and R. Gupta. SENSS: Security Enhancement to Symmetric Shared Memory Multiprocessors. *Proceedings of the 11th International Symposium on High-Performance Computer Architecture (HPCA'05)*, pp. 352-362, 2005.

[34] F.Y. Hou. "Research on Key Techniques of Memory System Data Confidentiality and Integrity Protection[Ph.D.dissertation]", *National University of Defense Technlology*, 2005. (侯方勇. 存储系统数据机密性与完整性保护的关键技术研究[博士学位论文], *国防科技大学*，2005.)

[35] C.Y. Yan, B. Rogers, D. Englender, Y. Solihin and M. Prvulovic. Improving Cost, Performance, and Security of Memory Encryption and Authentication. *Proceedings of the 33rd International Symposium on Computer Architecture(ISCA'06)*, pp.179-190, 2006.

[36] D.A. McGrew, J. Viega. The Security and Performance of the Galois/Counter Mode(GCM) of Operation. *5th International Conference on Cryptology(CRYPT'05)*, pp.343-355, 2005.

[37] C.H. Lu, T. Zhang, W.D. Shi and H.S. Lee. M-TREE : A high efficiency security architecture for protecting integrity and privacy of software. Journal of Parallel and Distributed Computing, vol.66, no.9, pp.116-128, 2006.

[38] R. Elbaz, L. Torres, G. Sassatelli, P. Guillemin, M. Bardouillet and A. Martinez. A Parallized Way to Provide Data Encryption and Integrity Checking on a Processor-Memory Bus. Proceedings of the 43rd annual Design Automation Conference(DAC'06), pp.506-509, 2006.

[39] S.C. Ma. "Research and Design on Real-Time Digital Security Chip[Ph.D.dissertation]" , *Institue of Computing Technology Chinese Academy of Sciences*, 2006.(马士超. 实时数字安全处理器研究与设计[博士学位论文], *中国科学院计算技术研究所*，2006.)

[40] L. Liu, H.W. Zou and Y. Tang. Research and implementation of programmable security processor. *Journal of Guangzhou University(Natural Science Edition)*, vol.5, no.4, pp. 54-57.(刘磊，邹候文，唐屹. 一种可编程安全处理器体系结构的研究与实现. *广州大学学报(自然科学版)[J]*, 2006, 5(4) :54-57.)

[41] W.D. Shi and H.S. Lee. Accelerating Memory Decryption and Authentication with Frequent Value Prediction. *Proceedings of the 4th International Conference on Computing Frontiers(CF'07)*. pp.35-46, 2007.

[42] B. Rogers, S. Chhabra, Y. Solihin and M. Prvulovic. Using Address Independent Seed Encryption and Bonsai Merke Trees to Make Secure Processors Os and Performance Friendly. *Proceedings of the 40th Annual International Sysposium on Microarchitecture(MICRO'07)*. pp.183-196, 2007.

[43] R. Elbaz, D. Champagne, R.B. Lee, L. Torres, G. Sassatelli and P. Guillemin. TEC-Tree : A Low-Cost, Parallelizable Tree for

Efficient Defense Against Memory Replay Attacks. *Cryptographic Hardware and Embedded Systems*. pp. 289-302, 2007.

[44] R.H. Lu, X.Y. Zeng, J. Han, Y.H. Gu and L. Mai. Design and VLSI Implementation of an Application Specific Instruction Set Security Processor. *Journal of Chinese Computer Systems*. vol.28, no.9, pp.1724-1728, 2007. (陆荣华，曾晓洋，韩军，顾叶华，麦浪. 专用指令集安全处理器设计与 VLSI 实现. *小型微型计算机系统[J]*. 2007, 28(9) :1724-1728.)

[45] L. Han, J. Han, X.Y. Zeng, R.H. Lu and J. Zhao. A programmable security processor for cryptography algorithms. *9th International Conference on Solid-State and Integrated-Circuit Technology (ICSICT'08)*. pp.2144-2147, 2008.

[46] R. Kannavara, N.G. Bourbakis, A. Dollas and P. Athanas. SCAN-Secure Processor. *2008 IEEE National Aerospace and Electronics Conference(INAEC'08)*. pp.219-224, 2008.

[47] R. Vaslin, G. Gogniat, J.P. Diguet, E. Wanderley and R. Tessier. A security approach for off-chip memory in embedded microprocessor systems. *Microprocessors and Microsystems*. vol.33, no.1, pp.37-45, 2009.

[48] A. Menezes, P.V. Oorschot and S.A. Vanstone. Handbook of Applied Cryptography. *CRC Press*, pp.23-45, 1996.

[49] J.A. Garay, V. Kolesnikov and R. Mclellan. MAC Precomputation with Application to Secure Memory. Information Security, no.5735, pp.427-442, 2009.

[50] M.Abramovici and P.Bradley, Integrated circuit security-new threats and solutions. *Proceedings of the 5th Annual Cyber Security and Information Intelligence Research Workshop*. 2009.

[51] ARM LIMITED. ARM Security Technology Building a Secure System using TrustZone Technology. *ARM Publication*, pp. 1-30, 2009.

[52] A. Rogers and A. Milenkovic. Security extensions for integrity and confidentiality in embedded processors. *Microprocessor & Microsystems*. vol.33, no.5, pp.398-414, 2009.

[53] B. Xia, Y.H. Bai and Q.S. Zheng. Research and Implementation of a Security Processor Based on Embedded Systems. J*ournal of Zhongyuan University of Technology*. vol.20, no.4, pp.19-21, 2009. (夏冰，白永红，郑秋生. 一种基于嵌入式系统的安全处理器研究与实现. *中原工学院学报[J]*. 2009, 20(4): 19-21.)

[54] L. Han, J. Han, X.Y. Zeng, R.H. Lu and J. Zhao. Architecture Design and VLSI Implementation of an Application Specific Instruction Set Security Processor. *Journal of Chinese Computer Systems*. vol.30, no.4, pp.746-751, 2009. (韩林, 韩军, 曾晓洋, 陆荣华, 赵佳. 一种专用指令集安全处理器的架构设计与 VLSI 实现. *小型微型计算机系统[J]*. 2009, 30(4): 746-751.)

[55] A. Waksman and S. Sethumadhavan. Tamper Evident Microprocessors. *2010 IEEE Symposium on Security and Privacy (SP'10)*, pp.173-188, 2010.

[56] H.X. Wang, G.Q. Bai and H.Y. Chen. Design of a high performance network security processor. *Journal of Tsing hua University(Science & Technology)*. vol.50, no.1, pp.13-17, 2010. (王海欣, 白国强，陈弘毅. 高性能网络安全处理器的设计. *清华大学学报（自然科学版）[J]*，2010, 50(1):13-17)

[57] J.M. Szefer, W. Zhang, Y.Y. Chen, D. Champagne, K. Chan, Will X.Y. Li, R.C.C. Cheung, R.B. Lee. Rapid-single-chip secure processor prototyping on the OpenSPARC FPGA platform. *2011 22nd IEEE International Symposium on Rapid System Prototyping (RSP'11)*, pp.38-44, 2011.

[58] P. Williams and R. Boivie. CPU Support for Secure Executables. *4th International Conference on Trust and Trustworthy Computing (TRUST'11)*, pp.172-187, 2011.

[59] S.A. Seyyedi, M. Kamal, H. Noori and S. Safari. Securing Embedded Processors against Power Analysis Based Side Channel Attacks Using Reconfigurable Architecture. 2011 IFIP 9th International Conference on Embedded and Ubiquitous Computing (EUC'11), pp.255-260, 2011.

[60] S. Wang, Y. Li, J.B. Liu, J. Han and X.Y. Zeng. A security processor based on MIPS 4KE architecture. *2011 IEEE 9th International Conference on ASIC (ASICON'11)*, pp.751-754, 2011.

[61] R.J. Wang. "The Research of Architecture Design and Implementaion of Security SoC ", *PLA Information Engineering University*, 2011.(王瑞蛟. 安全 SoC 体系结构的设计与实现研究[硕士学位论文], *解放军信息工程大学*，2011.)

[62] C.F. Deng. "Research of Secure Processor Architecture Based on Stream Cipher", *Chongqing University*, 2011.(邓程方. 基于流密码的安全处理器架构研究[硕士学位论文], *重庆大学*，2011.)

[63] S.Y. Cheng. Research on Memory Confidentiality and Integrity Protection Technology. Harbin Engineering University. 2012. (程顺毅. 存储器机密性完整性保护技术研究[硕士学位论文]. *哈尔滨工程大学*. 2012)

[64] D.Dubeuf and R. Karry, "Run-time detection of hardware Trojans: The processor protection unit," *IEEE Eur. Test Symp*, pp. 156–161, May 2013.

[65] R. Karri. Securing Processors Against Insider Attacks: A Circuit-MicroArchitecture Co-Design Approach. *IEEE Design & Test of Computer*, vol.30, no.2, pp.35-44, 2013.

[66] J.X. Zheng, D.F. Li and M. Potkonjak. A Secure and unclonable embedded system using instruction-level PUF authentication. *2014 24th International Conference on Field Programmable Logic and Applications (FPL'14)*, pp.1-4, 2014.

[67] C.H. Gebotys. Security-driven exploration of cryptography in DSP cores. *15th international Symposium on System Synthesis (ISSS'02)*, pp.80-85, 2002.

[68] Z.Q. He, X.R. Deng, B.M. Yang, K. Dai and X.C. Zou. A

SCA-resistant processor architecture based on random delay insertion. *2015 International Conference on Computing and Communications Technologies(ICCCT'15)*. pp.278-281. 2015.

[69] W.W Shan, X.Y. Fu and Z.P. Xu. A Secure Reconfigurable Crypto IC with Countermeasures Against SPA, DPA and EMA. *IEEE Tansactions on Computer-Aided Design of Integrated Circuits and Systems*. vol.34. no.7, pp.1201-1205, 2015.

[70] N.L. Zhu, S.Y. Qu and Z.B. Dai. Design of a Network Security Processor for Terminal Devices. *Microelectronics & Computer*. vol.32, no.12, pp.80-84. (朱宁龙，曲思源，戴紫彬. 面向终端的网络安全处理器体系结构设计. *微电子学与计算机[J]*. 2015, 32(12): 80-84.)

[71] D. Whelihan, K. Thurmer and M. Vai. A Key-centric Processor Architecture for Secure Computing. *2016 IEEE International Symposium on Hardware Oriented Security and Ttust(HOST'16)*, pp.173-178, 2016.

[72] E.M. Songhori, S. Zeitouni, G. Dessouky, T. Schneider, A.R. Sadehi and F. Koushanfar. GarbledCPU :A MIPS Processor for Secure Computation. *2016 53nd Design Automation Conference (DAC'16)*, pp.1-6, 2016.

[73] J.X Guo, L.J. Wu, Y. Niu, Z.Q. Wang, W. Jia and C. Zhang. An IPSec Accelerator for Online Network Security Processor SoC. *Microelectronics*, vol.46, no.1, pp.90-94,2016.(郭金星，乌力吉，牛赟，王自强，贾雯，张春. 一种在线网络安全处理器 SoC 的 IPSec 加速器. *微电子学[J]*. 2016, 46(1) :90-94.)

[74] B.CHEN and T. MORRIS. Certifying Program Execution with Secure Processors. *9th Hot Topics in Operating Systems (HotOS'03)*. pp.1-15, 2003.

赵剑锋 于 2006 年在北京理工大学通信与信息系统专业获得硕士学位。现在中国科学院信息工程研究所计算机系统结构专业攻读博士学位。研究领域为计算机系统安全。研究兴趣包括: 架构安全。Email: zhaojianfeng@iie.ac.cn

史岗 于 2004 年在中国科学院计算技术研究所获得博士学位。现任中国科学院信息工程研究所第五研究室高级工程师。研究领域为计算机系统安全。研究兴趣包括: 嵌入式系统、信息安全。Email: shigang@iie.ac.cn