

晶上系统广义功能安全技术研究综述

李沛杰, 郭威, 沈剑良, 曹志鹏, 梅波

(信息工程大学, 河南 郑州 450001)

摘要: 随着集成电路摩尔定律的逐步失效, 未来信息系统的技术物理形态将由集成芯片向集成系统发展, 晶上系统作为集成系统的一种, 相比2D/2.5D/3D集成芯片, 既有传统SoC芯片的逻辑结构和2.5D/3D异构集成电路工艺集成的微系统结构, 也有面向系统应用的软硬件协同结构, 呈现出功能安全、信息安全和网络安全融合交织的系统级广义功能安全问题, 现有2D/2.5D/3D IC芯片级的安全技术已难以满足。首先分析了2D/2.5D/3D IC的安全问题及从芯片上升到系统后现有芯片级安全技术的不足, 然后阐述了晶上系统广义功能安全问题产生的过程、面临的新挑战和新机遇。首次将晶上系统与网络空间内生安全理论结合, 提出一种晶上系统的广义功能安全威胁模型, 给出晶上系统广义功能安全技术的3个发展趋势。

关键词: 硬件木马; 广义功能安全; 动态异构冗余; 晶上系统; 异构集成

中图分类号: TP309.2

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025003

Survey on generalized safety and security technology for system on wafer

LI Peijie, GUO Wei, SHEN Jianliang, CAO Zhipeng, MEI Bo

Information Engineering University, Zhengzhou 450001, China

Abstract: With the failure of Moore's law in integrated circuits, the technical and physical form of information systems was expected to evolve from integrated chip (IC) to integrated system (IS). Compared to 2D/2.5D/3D IC, system on wafer (SoW), as one of the IS, was characterized by both the logic structures of system on chip (SoC) and the microsystem structures for 2.5D/3D heterogeneous IC, as well as the macrosystem structures for complex applications. The existing 2D/2.5D/3D IC chip-level security technologies were found to be insufficient in addressing the proposed generalized safety and security (GSS) problems, which included functional safety, information security, and cyberspace security. Firstly, the security problems of 2D/2.5D/3D IC were analyzed, and the shortcomings of the existing security technologies were identified with the transition from IC to IS. Then, the causes of GSS problems and the associated challenges were analyzed. A GSS threat model for SoW was proposed for the first time by integrating the SoW with the cyberspace endogenous safety and security theory. Additionally, the research progress of GSS tech-

收稿日期: 2024-06-29; 修回日期: 2024-11-24

通信作者: 李沛杰, lipeijie@csivo.com

基金项目: 国家重点研发计划 (2022YFB4401401, 2023YFB4404202)

Foundation Item: The National Key R&D Program of China (2022YFB4401401, 2023YFB4404202)

引用格式: 李沛杰, 郭威, 沈剑良, 等. 晶上系统广义功能安全技术研究综述[J]. 网络与信息安全学报, 2025, 11(1): 1-19.

Citation Format: LI P J, GUO W, SHEN J L, et al. Survey on generalized safety and security technology for system on wafer[J]. Chinese Journal of Network and Information Security, 2025, 11(1): 1-19.

nology was summarized. Finally, three development trends of GSS technology for SoW were outlined.

Keywords: hardware trojan, generalized safety and security, dynamic heterogeneous redundancy, system on wafer, heterogeneous integration

0 引言

集成电路 (integrated circuit, IC) 是现有信息系统技术物理形态的基础和核心, 以片上系统 (system on chip, SoC) 为代表的 2D IC 在物联网、工业控制、汽车电子及武器装备等系统中发挥着重要作用, IC 的安全问题直接影响系统的安全。随着集成电路技术的发展, 2.5D/3D 异构集成技术已经成为当前集成电路的新驱动技术。相比传统的 2D IC, 2.5D/3D IC 通过新集成工艺获得更高的集成密度和更丰富的功能特性, 同时带来了更加复杂的硬件安全问题。随着摩尔定律的逐步失效, 未来信息系统的技术物理形态将由集成芯片向集成系统转变^[1], 以大芯片为目标的传统 2D/2.5D/3D IC 不得不向以系统为目标的异构集成系统转变。

晶圆级集成作为异构集成技术的继承与发展, 可将 2D/2.5D/3D IC 集成在晶圆上, 实现更高的集成密度和集成效率, 晶上系统 (system on wafer, SoW)^[2]是以系统级应用为输入, 采用晶圆级集成技术将不同功能特性的裸芯集成在硅晶圆上形成的复杂应用系统。相比 2D/2.5D/3D IC, SoW 具有更高的集成密度和更典型的系统应用特性, 必然面临着比 2D IC 安全^[3-4]和 2.5D/3D IC 安全^[5-7]更复杂的安全问题。

1) 在硬件形态上, SoW 的物理结构使其安全问题不但继承了 2D/2.5D/3D IC 等裸芯的传统硬件安全问题, 而且新增的硅晶圆同样会引入硬件安全问题。与此同时, 高密度集成工艺特征使得 SoW 的不确定物理失效问题显著, 针对 SoW 的安全攻击更容易淹没在不确定物理失效中, 给 SoW 的安全检测与防御带来极大的挑战。

2) 在安全问题级别上, 现有的 SoC 和异构集成技术是大芯片拆分成小芯粒、小芯粒拼装成大芯片的技术路线, 从 2D IC 到 2.5D/3D IC 主要是从芯片器件维度带来的技术进步, 因此围绕 2D/2.5D/3D IC 安全问题的研究仍然是芯片器件级的, 重点集中在以保障芯片器件功能无故障运行

的功能安全和以保障 IC 设计数据和敏感信息数据可信的信息安全上。SoW 将器件维度上升到系统维度, 其内涵不单是晶圆上计算、网络、传感和物理环境的简单组合, 还包括整个软硬件系统和承载的应用, 是一种典型的信息物理系统 (cyber-physical system, CPS), 因此 SoW 的安全问题既要考虑其物理结构下特有的功能安全和信息安全问题, 也要关注整个软硬件系统与应用上所特有的网络空间安全问题^[8], 3 种安全问题相互交织且难以分而治之, 呈现出新质的广义功能安全 (generalized safety and security, GSS) 问题^[9]。

3) 在安全防御开销上, 受硬件资源限制, 2D/2.5D/3D IC 的安全防御只能在平衡功耗性能面积 (power-performance-area, PPA) 下进行器件级的轻量电路设计。而 SoW 丰富的硬件资源、为解决不确定物理失效而天然具备的动态异构冗余特性及系统级的架构优势, 使其安全防御可基于系统级安全架构设计, 借鉴网络空间内生安全理论^[8]的广义鲁棒控制技术^[10]一体化解决交织复杂的 SoW GSS 问题。

本文首先从 2D/2.5D/3D 等集成芯片的安全问题分析出发, 对现有集成芯片的威胁模型和安全问题进行总结, 指出当前围绕 2D/2.5D/3D IC 安全问题的研究不足; 然后分析了 SoW GSS 问题产生的原因、面临的挑战和机遇, 形成 SoW 特有的安全问题分类和 GSS 威胁模型, 并阐述了研究 SoW GSS 技术的意义。在此基础上, 对当前 SoW GSS 技术的研究进展进行全面分析, 指出 SoW GSS 技术当前研究进展的不足及未来的发展方向。

1 IC 的安全问题

1.1 2D IC 的安全问题

2D IC 一般由定制的逻辑电路和第三方 IP (逻辑 IP、存储 IP、外设 IP 等) 组成, 学术界对 2D IC 安全问题的研究由来已久^[11], 围绕 2D IC 的安全威胁主要包括物理安全威胁和逻辑安全威胁两类。物理安全威胁^[12-17]是以窃取 2D IC 芯片

电路结构信息为目的的安全问题; 逻辑安全威胁^[18-22]是以窃取片内敏感数据为目的的信息安全问题, 或以破坏芯片功能为目的的功能安全问题。随着集成电路微缩工艺的进步, 以窃取IC电路结构信息为目的的物理攻击越来越难以实现, 现有针对IC的安全问题主要以逻辑安全威胁为主, 如故障注入^[19]、侧信道攻击^[20-21]和硬件木马^[22]等。2D IC的逻辑安全问题在以片上网络(network on chip, NoC)为基础的SoC芯片上最为典型。基于NoC的SoC的结构如图1所示, 定制的逻辑电路和第三方IP通过NoC上的网络接口(network interface, NI)接入NoC, 并基于路由节点R实现所有逻辑的连接。

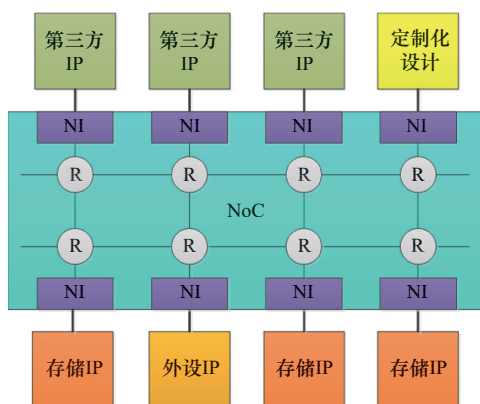


图1 基于NoC的SoC的结构

Figure 1 The structure of SoC based on NoC

SoC中的IP使用数据报文通过NoC进行信息的相互传递, 因此NoC可以看到IP之间交互的任何信息, 所有安全威胁均可通过NoC发起敏感信息窃听或逻辑功能破坏, 这些安全威胁包括基于不可信第三方IP的恶意植入^[23]、基于测试接口的后门威胁^[24]及基于定制逻辑电路的无意漏洞^[25]等。Charles等^[26]从安全攻击导致的结果分析, 将基于NoC的SoC所面临的安全威胁总结为信息窃取攻击^[27]、欺骗/数据完整性攻击^[28]、拒绝服务攻击(denial-of-service, DoS)^[29]、缓存溢出/内存提取攻击^[30]和侧信道攻击^[31]5种类型, 其安全威胁模型如图2所示。

1) 信息窃取攻击: 利用嵌入路由节点或者网络接口(如图2中①处)的硬件木马复制并篡改经过信息的目的地址, 使恶意IP窃取敏感信息; 通过对外的接口(如图2中②处)直接窃听。信

息窃取攻击几乎不损害SoC的功能安全, 可通过身份认证、敏感信息加密、报文复制监控和信息隐藏等手段进行安全防御。

2) 欺骗/数据完整性攻击: 与信息窃取攻击类似, 利用嵌入路由节点或者网络接口(如图2中③处)的硬件木马直接篡改经过信息的片段, 使得数据包损坏; 在通信链路上(如图2中④处)嵌入木马以篡改信息片段, 使得链路通信异常。欺骗/数据完整性攻击会损害SoC的功能安全, 可通过身份认证、ECC校验等手段进行安全防御。

3) DoS攻击: 利用嵌入路由或网络接口(如图2中⑤处)的硬件木马篡改路由信息或报文片段, 导致数据包异常占用网络资源, 从而发生拥塞; 利用嵌入IP(如图2中⑥处)的硬件木马注入报文, 导致拥塞。DoS攻击会损害SoC的功能安全, 可通过关键字段模糊化、区域划分与隔离、业务流量监控及异常检测等手段进行安全防御。

4) 缓存溢出/内存提取攻击: 一种专门针对多核处理器SoC共享内存的安全攻击, 恶意操控内存导致溢出以覆盖原有可执行代码程序(如图2中⑦处), 从而窃取敏感信息或进行异常控制。缓存溢出/内存提取攻击可能会带来信息安全和功能安全问题, 可通过授权访问控制、区域划分与隔离等手段进行安全防御。

5) 侧信道攻击: 通过分析安全芯片(如图2中⑧处)的非功能行为(如时间、延迟、功率等)侧面窃取安全密钥。侧信道攻击一般不损害SoC的功能安全, 可通过随机化路由、动态资源分配、应用任务随机化映射及业务流量动态分配等手段进行安全防御。

综上所述, 在2D IC安全威胁中, 攻击者以硬件木马或外部介入的方式对SoC中的交互信息进行攻击, 导致功能故障或信息泄露, 属于典型的功能安全问题或信息安全问题。

鉴于此, 2D IC的安全防御成为研究重点, 文献^[26]给出了以NoC为基础的SoC芯片在应对上述安全攻击时的防御机制, 其中在信息结构上, 通过在互连接口或路由节点部署访问控制、加密算法、防火墙、报文解析与监测等逻辑电路实现对传输信息的加密或监测。在系统结构上, 基于NoC, 通过安全区域划分、模糊设计

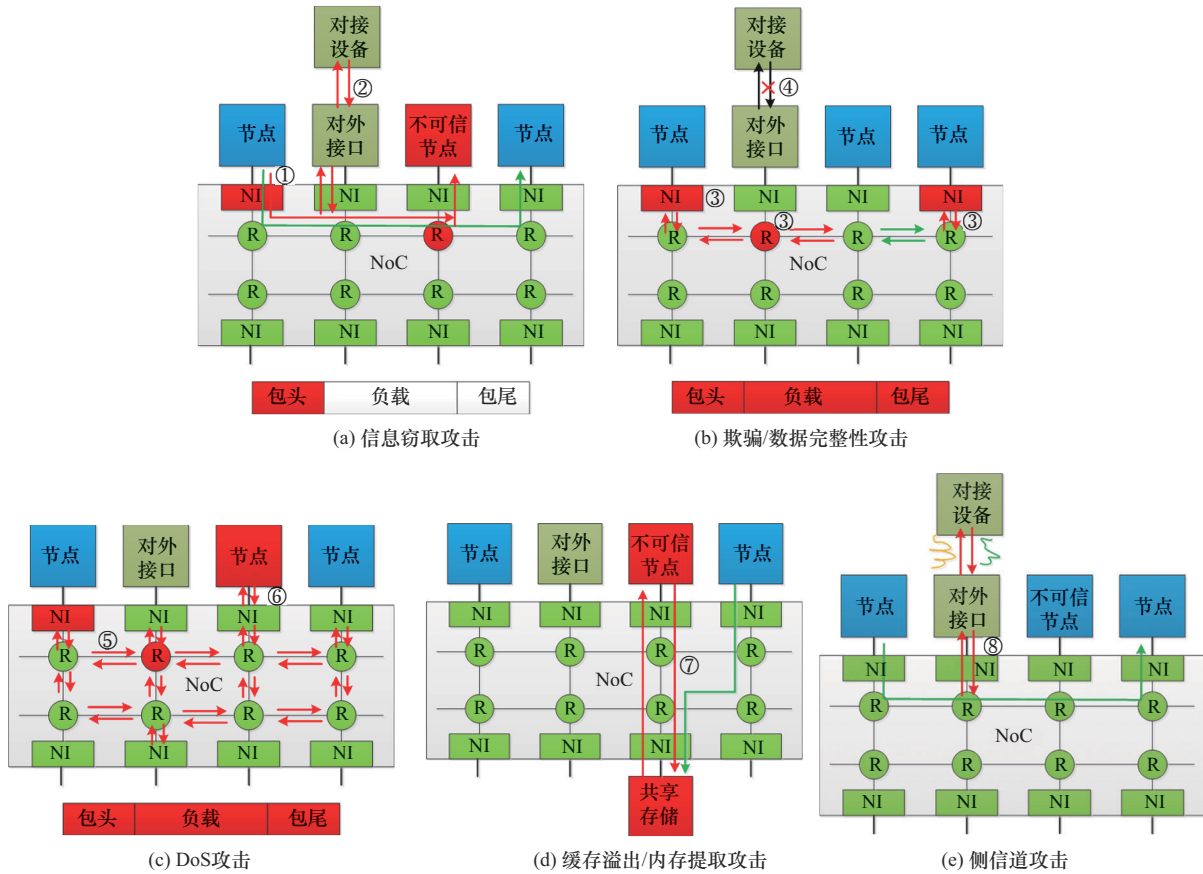


图 2 2D IC 安全威胁模型

Figure 2 2D IC security threat model

等防御机制, 提高信息传输的动态性和异构性, 增加攻击难度。在攻击检测与定位上, 新技术或新算法成为运行时安全防御的关键。文献[27]采用机器学习的方法对 DoS 攻击行为进行分析和训练, 并基于训练模型进行异常流量监测和攻击定位。文献[29]通过在路由节点上采用检测与定位算法, 实现对 DoS 攻击的实时检测与快速定位。整体来看, 以增加额外硬件资源进行加密或授权实现信息安全防护的方式本质上属于静态防御, 难以满足运行时多样化的安全需求, 而通过增加动态性或模糊设计实现的安全防御方法尽管具备一定的动态性, 但因资源受限, 仍然缺乏异构性和冗余性, 难以应对漏洞后门等内生的安全威胁。

1.2 2.5D/3D IC 的安全问题

随着摩尔定律的逐步失效, 传统 2D IC 的片上资源已不够用, 以 Chiplet 为代表的 2.5D/3D 异构集成技术^[32]迅速发展, 可实现系统级摩尔定

律延续, 解决 2D IC 的硬件资源问题。

2.5D/3D IC 的典型结构如图 3 所示。2.5D IC 通过硅正面和背面重布线层 (re-distribution layer, RDL) 及硅通孔 (through silicon via, TSV) 工艺形成硅转接板, 正面通过微凸点与不同工艺的 KGD (known good die) 连接, 背面通过 C4 凸点与有机基板连接。3D IC 的顶层一般采用先进工艺制备的逻辑 Die, 底部设计为存储 Die, 中间采用低工艺节点设计辅助 Die 或者硅转接板逻辑。3D IC 通过中间辅助 Die 将顶层逻辑 Die 和底部存储 Die 键合, 然后通过 C4 凸点与有机基板连接在一起。不同于 2D IC 将每个芯片单独封装在有机基板中, 2.5D/3D IC 通过引入新的硅转接板元素, 采用水平或者垂直互连的方式将不同工艺节点的多个 2D IC 集成在一起, 并封装在一个有机基板上^[33]。相比 2D IC, 2.5D/3D IC 采用小芯粒复用技术降低集成电路成本, 实现更多的功能。

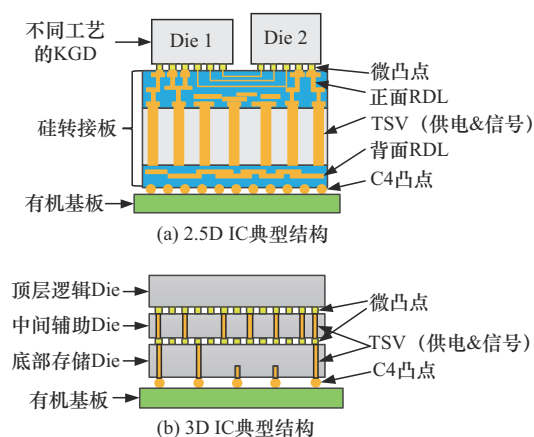


图3 2.5D/3D IC的典型结构
Figure 3 Typical structure of 2.5D/3D IC

2.5D/3D IC本质上是通过对新引入的工艺结构实现多个2D IC的拼装或堆叠。由于转接板的引入和典型应用下固定的异构集成模式，攻击者通过分析功能和用途不难确定2.5D/3D IC的基本结构，针对其中核心小芯粒或者转接板进行物理攻击即可实现对整个电路的攻击。因此，2.5D/3D IC尽管具有更高的集成密度，但仍是2D IC的延续，面临和2D IC相同的安全威胁，安全问题仍以破坏IC功能或窃取内部敏感信息为主。文献[7]总结了2.5D/3D IC除继承2D IC安全问题外所特有的安全问题，从攻击方式角度将其安全威胁模型归纳为逻辑攻击、物理攻击和结构攻击3类。在逻辑攻击方面，2.5D/3D IC与2D IC一致，特指IC被逻辑篡改而发生的DoS、机密信息泄露等，特别是由硅转接板带来的逻辑攻击问题。在物理攻击方面，与2D IC相比，2.5D/3D IC的攻击方式和难度略有变化。结构攻击是2.5D/3D IC特有的安全问题，指在

硅转接板的制备过程中，通过修改2.5D/3D IC的结构材料或者参数，使其绕过标准的可靠性测试，从而在必要时发起安全攻击，导致出现可靠性故障等功能安全。转接板的引入使2.5D/3D IC安全问题呈现新的特性。随着异构芯粒之间互连通道增多，通过恶意芯粒或转接板发起临近攻击更加容易，新结构的引入使得通过新元素（如TSV、微凸点、互连网络等）触发的功能安全问题更加突出。而高密度集成使针对IC的物理攻击变得更难。文献[34]从高密度集成结构考虑，指出2.5D/3D IC的测试和散热难题使恶意组件的检测难度和热侧信道攻击的风险增大，且2.5D/3D IC更容易在不同工艺环节和不同元素上插入硬件木马，利用热集中特征引入的热激活木马或者触发热可靠性异常的功能故障成为2.5D/3D IC所特有的安全问题。文献[35]和文献[36]从3D IC垂直结构的特殊性考虑，给出了垂直通信可信度、硬件特洛伊木马机制及新兴的侧信道攻击等3D IC特有的硬件安全威胁，并针对分离设计不同环节的硬件木马安全问题进行了总结，给出了比较全面的3D IC威胁模型。文献[37]从3D IC特有的部件考虑，给出3D IC中不同器件插入硬件木马的可能。文献[38]从威胁源和攻击目标出发，将3D IC的硬件特洛伊木马模型从2D IC单一硬件木马模型提升到跨层次木马触发、负载、协同攻击等硬件木马安全模型。

2.5D/3D IC与2D IC安全问题对比见表1。表2汇总了2.5D/3D IC的安全威胁模型。

从表1和表2可以看出，2.5D/3D IC继承了2D IC所有的物理安全和逻辑安全问题，在安全

表1 2.5D/3D IC与2D IC 安全问题对比
Table 1 Comparison of security issues between 2.5D/3D IC and 2D IC

条目	2D IC	2.5D/3D IC
威胁来源	不可信IP、不可信制造	恶意芯粒、转接板、不可靠元素
威胁类型	物理攻击、逻辑攻击	物理攻击、逻辑攻击、结构攻击
威胁触发特点	单一直接触发	协同间接触发、不可靠元素单一触发
物理攻击特点	以芯片为主，攻击难度大	以转接板为主，攻击难度小
逻辑攻击特点	以片内硬件木马触发为主，攻击难度大	以恶意芯粒通过互连接口侵入为主，攻击难度小
结构攻击特点	—	分离制造及不可靠结构多，攻击难度小
安全结果	以信息窃取和信息破坏为代表的信息安全	以故障触发硬件瘫痪为代表的功能安全

表 2 IC 的安全威胁模型
Table 2 Security threat model of IC

安全威胁来源	安全威胁类型	安全威胁	攻击触发机制	攻击导致结果	安全策略
芯粒安全	物理攻击	电路逆向	侧信道、电磁扫描、探针侵入等	物理信息泄露	物理屏蔽、电路模糊设计等
	逻辑攻击	信息窃取	硬件木马导致信息复制、基于测试接口的后门侵入	敏感信息泄露	信息加密
		欺骗/数据完整性攻击	硬件木马导致信息损坏	信息完整性	身份认证
		DoS	硬件木马导致信息损坏或异常注入	拥塞、功能瘫痪	区域划分与隔离、异常检测
		缓存溢出/内存提取	恶意内存访问	敏感信息泄露	访问控制
		侧信道攻击	热/功率/延迟等信息分析	敏感信息泄露	动态分配
转接板安全	物理攻击	电路逆向	侧信道、物理侵入+电磁扫描等	发起逻辑攻击和结构攻击	电路模糊设计、有源转接板
	逻辑攻击	信息窃取	恶意芯粒通过互连接口侵入、硬件木马协同	敏感信息泄露	信息加密、有源转接板
		欺骗/数据完整性攻击	路由节点或网络接口硬件木马	信息完整性	身份认证、有源转接板
		DoS	恶意芯粒通过互连接口侵入路由节点或网络接口木马	拥塞、功能瘫痪	区域划分与隔离、有源转接板
结构安全	逻辑攻击	侧信道攻击	局部热/功率/延迟等信息分析	发起逻辑攻击和结构攻击、敏感信息泄露	电路模糊设计、有源转接板
	结构攻击	组装侵入	组装时埋入传感器、电阻器件等	功能瘫痪、敏感信息泄露	区域划分与隔离
		硬件木马	基于铜布线、TSV的热触发	功能瘫痪	可靠性检测、冗余设计

攻击触发机制上与 2D IC 明显不同。相比 2D IC, 2.5D/3D IC 从基于 IP 的设计升级到基于芯粒的设计, 除继承芯粒内不可信 IP、分离设计制造导致的安全威胁, 还增加了由新引入转接板元素导致的安全威胁, 2.5D/3D IC 的安全威胁倍数级提升; 同时, 由于高密度拼装集成和垂直互连等结构性变化, 攻击者可利用新增的不可靠元素(如 TSV)进行安全攻击。此外, 测试难题、散热难题、不可靠工艺及元素等触发故障, 导致硬件瘫痪成为 2.5D/3D IC 面临的一个重要安全威胁。但总体来看, 2.5D/3D IC 在生产过程中由不确定物理失效导致的功能安全问题逐渐和由安全攻击导致的逻辑安全问题融合, 防御者难以脱离功能安全制定单一的逻辑安全防御措施。

新结构的引入同时给安全防御策略的灵活部署带来了可能。从表 2 可以看出, 现有针对 2.5D/3D IC 安全防御的研究主要围绕转接板和异构集成结构展开。在基于转接板的安全防御研究上,

文献[5]通过在有源转接板上构建一种与芯粒物理隔离的互连结构, 使芯粒在运行时依然被监测, 以保障芯粒间通信的信息安全。文献[35]依托有源转接板设计 3D 垂直通信的 NoC 互连网络, 通过结构和物理冗余设计对有源转接板进行保护。文献[39]在有源转接板上设计了安全控制平面对计算平面的所有通信、内存访问和共享信号进行检查和控制, 但这使得计算平面的所有芯粒必须匹配修改。文献[6]和[40]在假设垂直互连转接板设计及制备均可信的前提下, 利用 3D IC 的分离制造优势和互连网络结构, 设计了屏蔽电路和混淆电路, 分别应对针对转接板的物理攻击和恶意芯粒触发的临近攻击。在基于架构设计的安全防御研究上, 文献[41]通过增加异构冗余芯粒对核心芯粒进行保护, 以面积和性能损失换取核心芯粒安全。文献[42]针对硬件安全策略带来的面积和性能开销问题, 采用非硬件冗余和架构优化的方式, 创建和并行执行多种异构的特洛

伊木马感知软件变体,通过投票表决实现不受信任商用芯片运行时的特洛伊木马检测和恢复。这种方法同样适用于异构集成系统。文献[43]针对3D IC的跨层次硬件木马检测与应对难题,特别是系统运行时的检测问题,将3D IC的架构设计与安全机制统一考虑,通过在3D NoC的路由节点上部署特定检测电路实现对3D IC电路的硬件木马检测与定位。

整体来看,现有的2.5D/3D IC安全防护技术研究工作聚焦于两个方面:①采用有源设计构建互连网络屏蔽芯粒之间的互连关系,基于2D IC的安全策略解决异构集成芯片的安全问题;②采用增加硬件或软件资源的方式,通过异构、冗余、动态等架构优化技术实现安全防护。相比2D IC,2.5D/3D IC的安全防护可调用的资源更多,因此通过增加资源部署异构、冗余、动态的安全策略效果会更好。由于功能安全和逻辑安全问题的融合,安全策略的部署和功能需求下的设计重合,如有源转接板上的互连网络可能同时兼顾功能互连和安全互连的作用。但与2D IC一致,默认有源转接板可信进行的安全策略部署,同样无法保障安全策略逻辑是否存在内生的安全问题。

综上所述,现有围绕2D/2.5D/3D IC安全问题的研究要么以保障无故障运行的功能安全为目的,要么以保障IC设计数据和信息数据可靠的信息安全为目的。分离设计和高密度集成使测试工作变得困难,尤其是2.5D/3D IC在制备过程中引入的生产故障很难与安全攻击带来的功能故障区分。同样,以窃取和破坏信息为目标的安全攻击往往会带来功能故障,功能安全和信息安全逐渐交织。但总体来看,现有研究仍然停留在芯片器件层面,围绕硬件安全展开,没有从系统应用层面考虑因未知漏洞或后门等引入的网络空间安全问题。这是因为当前研究的对象仍然是异构集成芯片而非系统,随着集成芯片逐渐向系统发展,技术物理形态的变化必然使网络空间安全问题成为核心问题,功能安全、信息安全和网络安全的交织将更加突出。尽管部分研究通过增加动态、异构、冗余特性能够有效解决对应的安全问题,但受限于器件的PPA开销,集成芯片的安

全防御同样只能采用轻量级设计,难以有效构建系统级的安全防护。

2 SoW GSS问题

2.1 SoW GSS问题的产生

从微电子的技术发展趋势来看,集成电路只是手段,系统才是目的^[1],未来信息系统基础设施的技术物理形态必然向系统转变,集成电路的安全问题必然从集成芯片安全向集成系统安全发展。SoW作为集成系统的一种,以硅晶圆作为互连底座,集成各种功能芯粒组成核心单元,采用先进集成技术组装供电、散热、I/O接口和核心单元以实现特定功能。SoW的基本结构如图4所示。

从物理结构的改变来看,SoW首先在硅晶圆基板上实现有源或无源的互连网络,然后在其上贴装2D/2.5D/3D的IC芯粒,最后通过先进集成技术与供电、散热、I/O接口等组装在一起。SoW具有超高的集成密度,集成了来自不同第三方的百数量级芯粒,芯粒间间距极小,晶圆基板上集成了百万级微凸点^[44],因此SoW天然具有集成电路微系统的工艺特性和数量级倍增的资源规模。在继承性上,所有异构资源的不可信或者安全问题均会被继承,成为系统安全短板。在物理组成上,硅晶圆基板、供电、散热、微组装转接板等结构和工艺环节的引入,使得攻击者具有更多的攻击点和攻击手段触发SoW的硬件安全问题。由于集成规模更大,在生产、加工、集成等过程中不可避免会引入连线及功能单元的不确定物理失效问题,且继承和新增的安全问题会被转化放大(如相同厂商芯粒可能协同导致安全问题,互连接口导致的临近攻击问题)。

从逻辑结构的改变来看,SoW基于承载的软件系统及硅晶圆上的晶上互连网络(network on wafer, NoW),根据不同应用在硬件系统上灵活部署匹配的任务并协同处理,具有系统级的应用特性^[45]。SoW承载的不同任务在不同时刻会呈现服务的高动态特性,这种高动态特性使得SoW的应用安全问题不可查、不可预警,可在集成电路的任何环节(EDA工具、芯粒设计的IC公司、代工厂、硅晶圆基板设计、应用软件、处理的业务等)触发,也可在高动态的

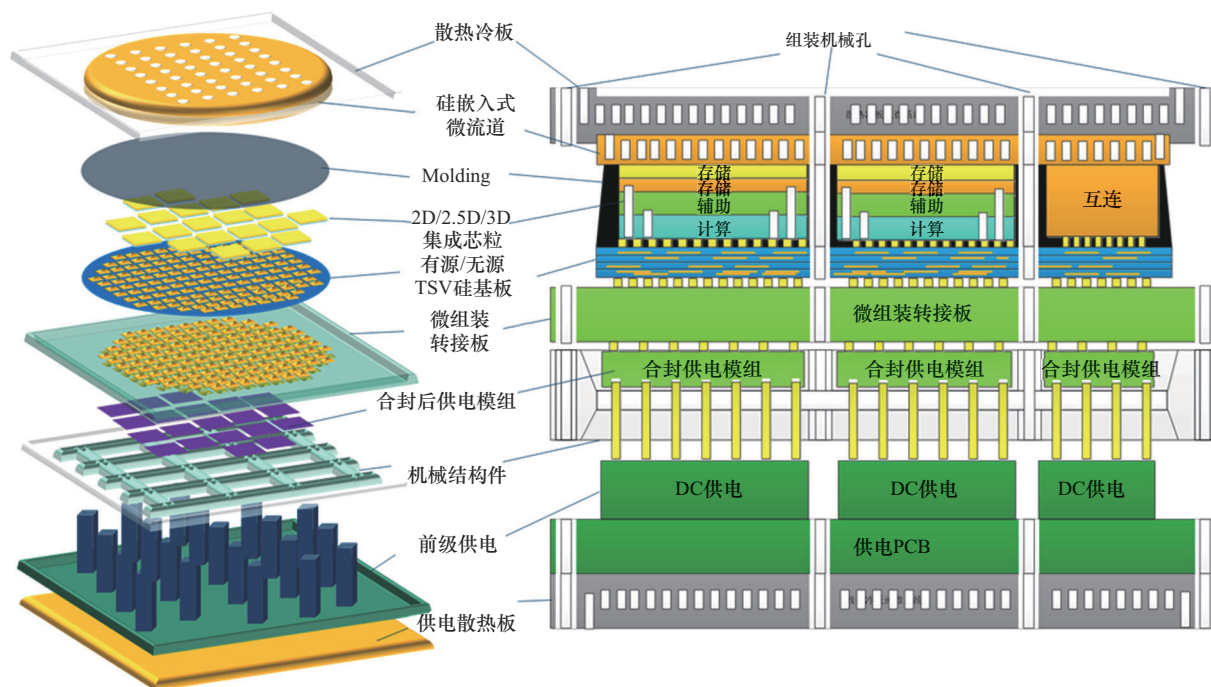


图 4 SoW 的基本结构

Figure 4 Basic structure of SoW

应用部署和任务协同时通过已知或未知的漏洞、后门触发，且由于大规模的集成与高动态的应用融合在一起，安全攻击的结果很难与不确定物理失效的结果区分。

从技术物理形态的改变来看，与 2D 的 SoC 相比，SoW 将一个光罩尺寸的物理限制提升到整个晶圆，集成规模更大；与 2.5D IC 相比，SoW 将整个系统从 PCB 形态提升到晶圆级形态，功能密度^[46]更高；与 3D IC 相比，SoW 将局部受限的面积和单芯片的功能提升到整个系统，在二维

面积和功能密度上均获得提升。不同于基于传统“裸 Die-封装-板卡-机匣-机箱-机架”层层堆叠模式实现的集成芯片技术物理形态，SoW 通过异构集成，实现特定的系统级应用部署，其本质是应用系统的晶圆级实现，因此 SoW 的安全问题不再是面向芯片的硬件安全，而是面向系统的硬件安全和应用安全的总和。

表 3 对 SoW 和 IC 的安全问题进行了对比。不同于集成电路和集成芯片，SoW 具有更复杂的安全问题，其中在物理结构上由大量芯粒及

表 3 SoW 与 IC 的安全问题对比

Table 3 Comparison of security issues between SoW and IC

条目	2D IC	2.5D/3D IC	SoW
技术路线	集成电路	集成芯片	集成系统
物理结构	更多晶体管	更大芯片，不可靠元素	更大系统，更多不可靠元素
逻辑结构	IP+NoC	小芯粒+转接板	软件+硬件
安全问题	芯片级	芯片级	系统级
威胁来源	不可信 IP、不可信制造	恶意芯粒、转接板、不可靠元素	恶意芯粒、晶圆基板、不可靠元素、漏洞和后门
不可靠元素	IP	芯粒、布线、TSV	芯粒、布线、TSV、供电、散热、软件、组装
威胁类型	以信息安全为主	以功能安全为主	以系统安全为主
威胁触发特点	单一直接触发	协同间接触发、不可靠元素单一触发	协同融合触发
安全设计	片内资源受限，轻量型	转接板资源受限，针对型	资源丰富，灵活型

不可靠元素组合形成的复杂系统中，任何芯粒或元素的安全问题都会迅速蔓延至整个系统，使SoW的安全问题呈指数级增长，由不可靠元素的不确定物理失效导致的功能安全问题更严重。恶意芯粒通过互连接口触发逻辑攻击，成为触发信息安全问题的主因，而侧信道攻击更加困难。此外，由于系统应用的部署，攻击者可利用系统级应用的漏洞、后门触发安全攻击，系统结构 and 应用随之带来了系统级的网络空间安全威胁。

总体来看，随着SoW在物理结构、逻辑结构和技术物理形态上的改变，其安全问题也随之改变：一是继承2D/2.5D/3D IC及引入新结构和新工艺后导致的硬件安全问题，如硬件木马、临近攻击等；二是由SoW软硬件设计与制造过程中的不确定物理失效带来的功能安全问题，如凸点开裂、热应力故障、软件漏洞等；三是在应用过程中通过NoW触发的软硬件及系统的内生安全问题，如漏洞、后门等。SoW的功能安全、信息安全和网络安全问题交织融合，形成了SoW

的GSS问题。

2.2 SoW GSS威胁模型

SoW GSS问题是一种交织融合的复杂安全问题，触发威胁的原因既有已知的硬件木马等芯片安全威胁，也有未知的漏洞、后门等网络安全威胁，威胁导致的结果既有可收集和分析的逻辑安全，也有不可预知的网络安全。SoW的不确定物理失效的结构问题及业务的高动态应用特征，使得针对SoW的安全攻击往往淹没在物理失效和动态应用中，极难从安全结果溯源威胁来源，同时存在难以预知安全结果的可能，这与文献[47]将网络安全威胁级别及各自安全模型划分为已知的已知（known knowns, KK）、已知的未知（known unknowns, KU）、未知的已知（unknown knowns, UK）和未知的未知（unknown unknowns, UU）一致。因此本文参照上述网络安全问题及属性的分类方法构建和完善SoW GSS威胁模型。SoW GSS威胁模型如图5所示，包括功能安全、信息安全和网络安全3个部分，且3类安全问题交织形成7个不同区域。

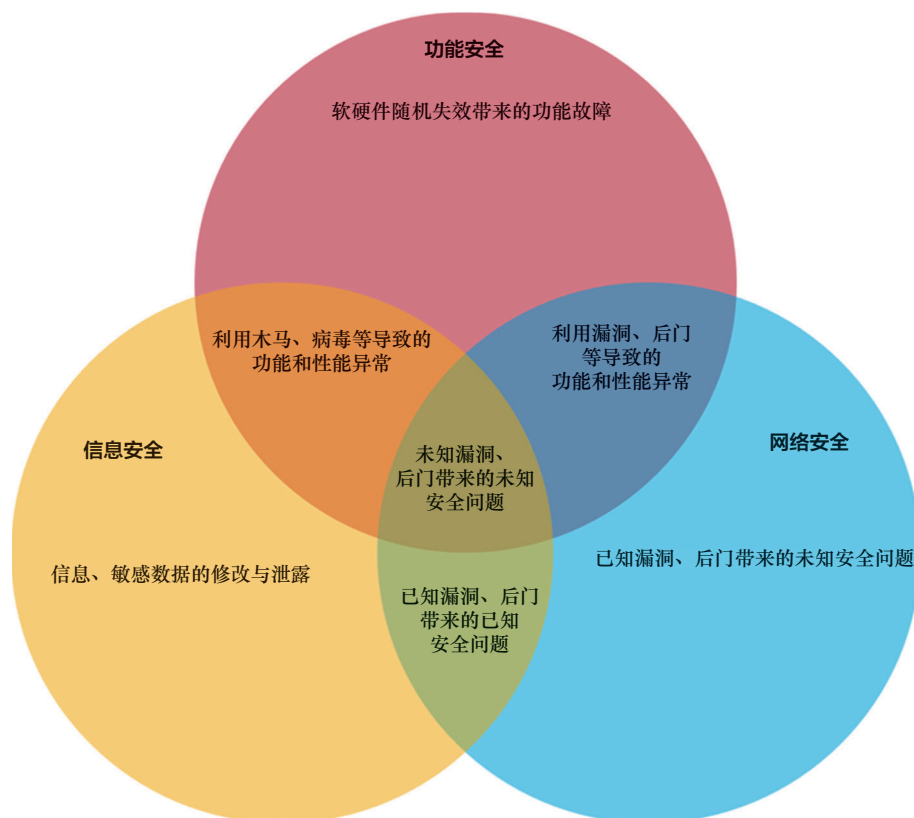


图5 SoW GSS威胁模型

Figure 5 SoW GSS threat model

1) 功能安全。指 SoW 各部件不确定物理失效或软硬件设计缺陷导致的随机故障, 这种随机故障会给系统的功能或性能造成损伤, 且具有随机性。造成安全问题的原因和机理相对清楚 (例如, 晶圆基板制备、微组装等工艺生产或不可信工艺环节嵌入硬件木马等带来的物理失效, 系统运行时因热、翘曲、应力等引发的可靠性物理失效, 软件设计缺陷导致的功能异常等), 导致的后果相对清楚但不可控, 可通过系统级的容错提升系统鲁棒性。

2) 信息安全。指 SoW 系统特性导致的信息、敏感数据的修改 (包括删除、增加或修改) 和泄露。这种安全攻击具有主动性, 造成安全问题的原因和机理及导致的后果相对清楚 (例如, 恶意节点通过高密度互连接口触发的信息泄露、信息劫持, 依赖系统健康监测等发起的侧信道攻击等), 可采用对应的安全策略进行防护。

3) 网络安全。指已知的漏洞、后门导致的 SoW 中 NoW 互连网络信息 (路由、域名、IP 等) 或网络设备 (NoW 的节点等) 未知安全问题。这种安全攻击具有主动性, 造成安全问题的原因和机理相对清楚 (例如, 嵌入晶上互连网络路由节点、网络接口或芯粒中的后门、硬件木马等), 但导致的后果和攻击触发的时机具有随机性和不确定性, 需要依赖已知的信息和分析进行威胁匹配。这种安全问题因为没有足够的结果数据, 因此很难进行针对性的“封门补漏”。

4) 功能安全与信息安全融合。指木马等病毒通过触发 SoW 内部敏感数据泄露或信息修改导致的功能和性能异常。这种安全问题具有主动性, 造成安全问题的原因 (如勒索、热触发木马、单一芯粒硬件木马等) 及导致的结果相对清楚, 可通过制定针对性的安全措施进行检测与防护。

5) 功能安全与网络安全融合。指通过已知的漏洞、后门等网络攻击触发的 SoW 系统中软硬件功能故障问题。这种安全问题具有主动性, 造成安全问题的原因和机理、导致的结果相对清楚 (如网络风暴、DoS 攻击等), 可通过针对性“封

门补漏”方式进行安全措施的制定与防护。

6) 信息安全与网络安全融合。指通过已知漏洞或后门等触发的 SoW 系统内部敏感数据及信息泄露或修改, 这种安全问题具有主动性和随机性, 造成安全问题的原因和机理清楚 (如恶意软件、跨芯粒的硬件木马协同等), 导致的结果相对清楚, 可采用通用的网络安全策略进行防护。

7) 功能安全、信息安全与网络安全融合。指通过未知漏洞、后门等触发的未知的安全问题, 这种安全问题具有主动性和随机性, 造成安全问题的原因和机理及导致的结果均不清楚, 甚至不知道是否存在安全问题, 现有的安全措施很难进行防护。

表 4 对 SoW GSS 威胁模型进行了整体描述。SoW GSS 不仅继承了 IC 的所有安全问题, 同时展现出两个特点: ①从安全威胁来源来看, 不确定物理失效导致的功能安全问题更加突出, 软硬件协同、多芯粒协同等系统级协同攻击成为主流; ②从攻击导致的结果来看, 难以根据结果溯源安全威胁的类型, 需要一体化解决 SoW 交织融合的 GSS 问题。

从表 4 可以看出, 恶意芯粒发起的临近攻击和同构恶意芯粒发起的协同攻击是 SoW 芯粒安全攻击的主要机制。图 6 (a) 所示为恶意芯粒发起的临近攻击, 恶意芯粒借助芯粒间的高密度互连接口接入互连网络, 利用互连接口中嵌入的硬件木马触发, 既可以在最小限度影响交互信息和网络特性时灵活发起信息攻击, 又可爆发式发起致瘫攻击。图 6 (b) 所示为同构恶意芯粒发起的协同攻击, 芯粒通过任意条件触发物理故障, 系统在功能异常下会启用故障恢复机制使信息修改传输路径到冗余通道, 此时同构的恶意芯粒借机发起攻击。

晶圆基板攻击和结构攻击是 SoW 最主要的硬件安全威胁来源。其中, 由有源晶圆基板或无源晶圆基板构建的晶上互连网络, 承担 SoW 的业务、管理、配置和时钟的传递, 针对晶上互连网络的安全攻击具有芯粒硬件安全威胁的所有特征, 可通过硬件木马、数据接口或应用程序后门与未知漏洞等对互连接口或路由节点发起攻击。

表4 SoW GSS威胁模型
Table 4 SoW GSS threat model

安全威胁来源	安全威胁类型	安全威胁	攻击触发机制	攻击导致结果	安全防御策略
芯粒安全	物理攻击	与IC一致	与IC一致	信息安全	与IC一致
	逻辑攻击	与IC一致	同构芯粒协同攻击、恶意芯粒发起临近攻击	信息安全 功能安全	与IC一致 安全互连接口
晶圆基板安全	物理攻击	与IC一致	与IC一致	信息安全	与IC一致
		与IC一致	与IC一致	信息安全 功能安全	与IC一致
		数据网络攻击	硬件木马触发、数据接口或应用利用程序后门入侵、利用未知漏洞对节点和互连接口发起攻击	信息安全 功能安全 网络安全	与规避功能故障一致的动态异构冗余设计
	逻辑攻击	管理网络攻击	硬件木马触发、管理接口或应用利用程序后门入侵、利用未知漏洞对节点和互连接口发起攻击	信息安全 功能安全 网络安全	动态异构冗余设计、模糊设计
		配置网络攻击	硬件木马触发、数据接口或应用利用程序后门入侵、利用未知漏洞对互连接口发起攻击	信息安全 功能安全 网络安全	动态异构冗余设计、模糊设计
		时钟网络攻击	硬件木马触发、系统接口后门入侵	功能安全	与规避功能故障一致的冗余设计
结构安全	逻辑攻击	侧信道攻击	与IC一致 通过供电、散热系统信息分析	信息安全	与IC一致
		组装侵入	与IC一致	信息安全 功能安全	与IC一致
	结构攻击	硬件木马	铜布线、TSV、微连接件、散热流道、供电等	功能安全	与IC一致
		供电系统入侵	网络入侵供电芯片	功能安全	系统级网络空间安全防御
应用安全	逻辑攻击	应用程序与部件攻击	应用漏洞、数据库、内存、窃听等	信息安全 功能安全 网络安全	新的网络空间内生安全防御

晶上互连网络的逻辑结构具有多维多模态的特征，可用于系统应用中已知和未知安全攻击下的安全防御。鉴于SoW GSS的特性，基于NoW的安全防御可与功能故障规避机制统一通过动态NI、多维路径异构冗余等设计，一体化解决SoW GSS安全问题，SoW的典型晶圆基板威胁模型如图7所示。

应用攻击是SoW特有的安全威胁。同晶圆基板安全威胁一样，利用应用程序漏洞、数据库、内存等发起攻击，致使应用程序或部件异常，与功能故障具有融合特性。安全威胁的触发和安全攻击导致的结果难以预知，传统的硬件安全防御策略难以有效解决，需要借助网络空间内生安全防御技术在SoW构建动态异构冗余的系统级安全架构。

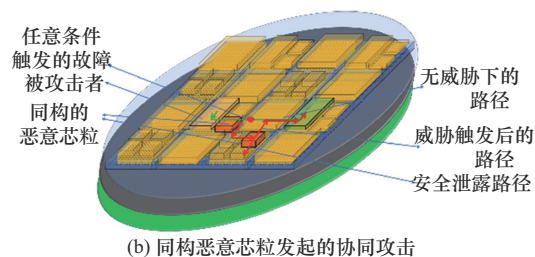
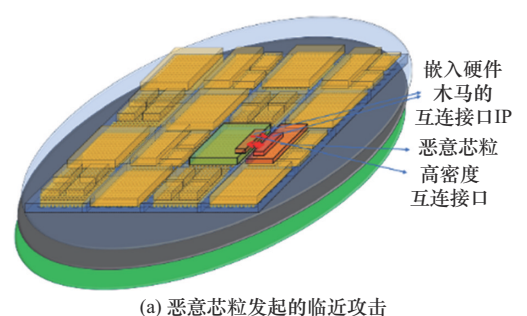


图6 SoW的典型芯粒威胁模型

Figure 6 Typical chiplet threat model of SoW

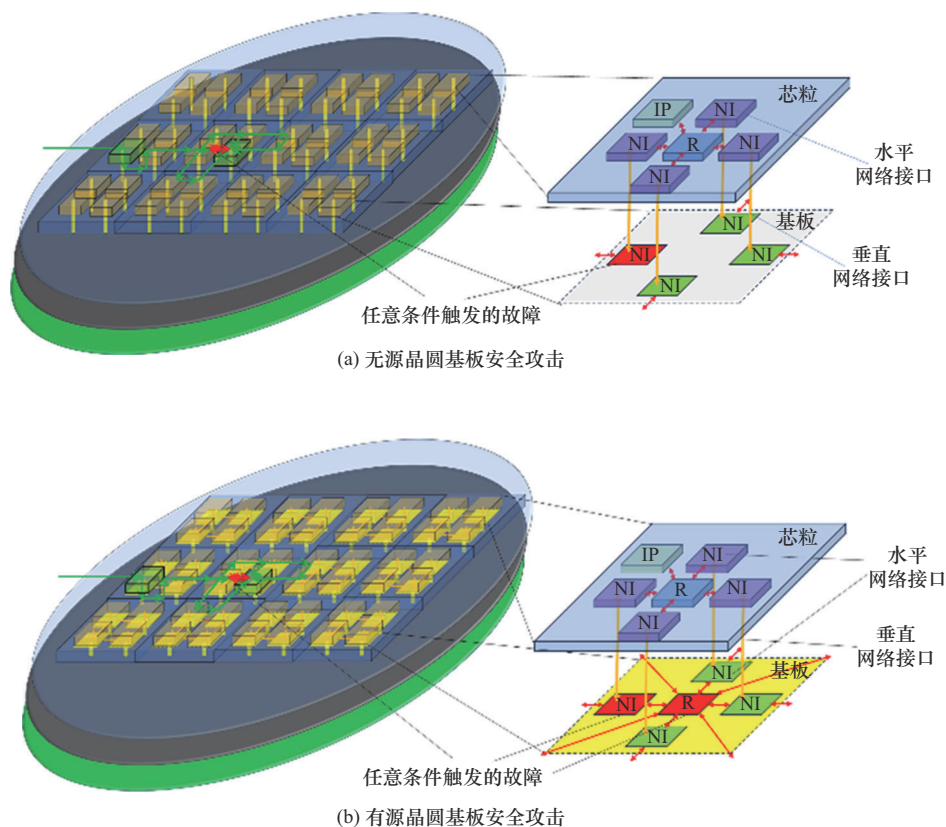


图 7 SoW 的典型晶圆基板威胁模型

Figure 7 Typical wafer substrate threat model of SoW

2.3 SoW GSS 技术研究挑战

由 SoW 呈现出的 GSS 威胁特征可以看出, 传统围绕 IC 的芯片级硬件安全技术不再适用, 需要新的系统级的安全技术。SoW GSS 防御技术研究面临下列挑战。

(1) 安全威胁的多样性给威胁检测带来了挑战

SoW 面临的安全威胁具有多样性。在硬件安全威胁方面, 既要面对继承 2D/2.5D/3D IC 的安全威胁, 又要面对引入硅晶圆、供电、散热等组件所带来的新的安全威胁。同时, 系统高密度互连结构引入了芯粒安全威胁, 包括协同攻击和临近攻击。此外, 系统高动态应用特性带来了特有的应用安全威胁, 包括已知或未知的应用漏洞和后门导致的应用安全攻击。这些威胁交织融合, 使得 SoW 的安全威胁更具隐蔽性, 攻击者往往更容易淹没在高密度集成导致的不确定物理失效中。此外, 未知的漏洞、后门带来的未知安全威胁问题更加突出。这些都给 SoW GSS 的威胁检

测带来了极大的挑战。

(2) 安全攻击的不确定性给安全防御带来了挑战

随着技术物理形态从芯片级向系统级转变, SoW 作为一种典型的 CPS, 其安全攻击所呈现出来的不确定性更加明显。既有基于已知的不确定扰动发起的硬件安全攻击, 也有基于未知的不确定扰动发起的网络攻击。此外, 系统级安全威胁来源的多样性和复杂性, 使得安全攻击的时间和空间都不确定。因此, 传统芯片级的点对点或封门补漏的安全防御方法难以应对 SoW GSS 威胁。GSS 威胁的交织融合特性, 使得 SoW 的安全防御难以分而治之, 需要研究系统级一体化的安全防御技术。

(3) 系统级安全防御在开销方面面临挑战

传统 2D/2.5D/3D IC 由于硬件资源受限, 其芯片级的安全防御方法更多采用轻量级的电路设计。SoW 集成规模更大, 如果按照传统芯片级的安全防御方法堆砌安全策略, 仅芯粒硬件安全防

御所带来的开销就会呈倍数级增长, GSS 安全防护开销显然更大, 因此必须构建系统级的安全防护方法。面对 GSS 威胁交织融合的特性, 如何构建高效、完备且开销可接受的系统级安全防护系统成为 SoW GSS 防御技术研究的一大挑战。

2.4 SoW GSS 技术研究意义

作为未来信息系统的新技术物理形态, SoW 属于一种面向特定应用的不确定系统, 其 GSS 问题不仅包含软硬件已知的不确定扰动(如随机物理失效以及已知的病毒、漏洞、后门等)和未知的不确定扰动(如未知的漏洞、后门等)导致的安全攻击, 还包括系统应用已知的不确定扰动(如应用的高动态部署)和未知的不确定扰动(如应用程序攻击等)导致的功能问题。但 SoW 丰富的硬件资源、为解决不确定物理失效而天然具备的动态异构冗余特性以及系统级的架构优势, 使得 SoW GSS 的安全挑战可转化为 SoW GSS 安全技术的优势, 研究 SoW GSS 技术可以有效解决 SoW GSS 问题。

1) 统一考虑 SoW 的各类安全问题, 弱化对安全问题原因和导致结果的强依赖, 有望一体化解决试错式或隧道穿越攻击难题和未知不确定扰动带来的未知安全问题, 确保 SoW 形态 CPS 的安全可靠。

2) 融合 SoW 的资源优势和动态异构冗余结构的构造优势, 可借助网络空间内生安全技术重构 SoW 架构, 有效解决安全措施构建、动态业务部署和资源占用之间的矛盾, 促进 SoW 安全架构技术发展。

3) 最大限度复用当前通信系统的鲁棒控制技术和 2D/2.5D/3D IC 的安全防护措施, 在 SoW 上构建 GSS 架构, 通过感知不同部件的扰动实现安全问题的定位或定性。

3 SoW 鲁棒控制技术研究现状

SoW 属于一种面向特定应用的不确定系统, 其安全问题是一种典型的 GSS 问题, 与网络空间的内生安全问题相似, 因此可采用拟态防御和广义鲁棒控制技术解决 SoW GSS 问题。SoW 属于新生的集成系统形态, 当前学术界和产业界的研究工作聚焦于 SoW 的工艺技术、通用架构技术和系统应用技术, 在安全技术方面更多是针对

SoW 不确定物理实现问题开展的鲁棒控制技术研究。SoW GSS 交织融合的特性, 使得针对 SoW GSS 的攻击往往淹没在不确定物理失效导致的功能安全问题中。现有针对 SoW 鲁棒控制技术研究, 可作为未来解决 SoW GSS 问题的基础。鉴于此, 追踪并总结 SoW 鲁棒控制技术的最新进展, 对未来 SoW GSS 技术的发展意义重大。

SoW 鲁棒控制技术研究工作着重于两个方面: 一是 SoW 工艺鲁棒控制技术研究, 二是系统级鲁棒控制技术研究。

3.1 SoW 工艺鲁棒控制技术

SoW 工艺鲁棒控制技术研究工作致力于解决 SoW 制备过程中的不确定性物理失效问题。现有的研究工作着重于工程实现和理论研究。在工程实现上, Cerebras 的 WSE (wafer scale engine) 和 Tesla 的 DOJO 走在前沿。WSE 采用冗余设计思路^[48], 在晶圆级大芯片前道生产工艺完成后, 首先基于传统芯片的筛选测试筛选出故障芯片, 然后在故障芯片附近选择好的芯片, 最后进行光罩之间再布线, 实现故障芯片冗余替换。故障芯片的筛选及再布线后功能故障的检测成为其应对结构安全的关键。Tesla 的 DOJO 通过简化互连拓扑, 在 2D-mesh 硬件结构基础上, 通过软件控制路由规避系统中的故障芯片^[49] (故障芯片不再被使用)。贴装在晶圆上的芯片是经过筛选测试的 KGD, 因此这种故障主要存在于芯片和晶圆键合过程或者使用过程中的不确定性扰动。显而易见, SoW 采用三维异构集成技术路线, 系统的可靠性问题主要表现为晶圆基板在制备过程中的工艺随机性失效、芯粒与晶圆基板贴装过程中的连接随机性失效、系统在微组装或者组装过程中的集成随机性失效及运行时的不确定性扰动。围绕这些不可信问题, 学术界开展了很多的研究工作, 其中, 以 UCLA 为代表的 Si-IF (silicon interconnect fabric) 侧重于工艺实现过程的可靠性保障。文献[50-51]指出热效应、机械振动、湿度和污染都会导致 SoW 失效。其中, 热效应和机械振动导致的失效主要表现为结构疲劳失效、焊点疲劳失效和过度变形失效, 这两类原因导致的失效占整体失效的 75%; 针对热失效问题,

文献[52]给出了一种低温晶圆到晶圆熔合工艺,用于增强焊点键合的可靠性。文献[53]通过解决初始表面粗糙度、化学机械抛光、粘合压力和温度的作用来实现 Au-Au 键合的可靠性。文献[54]通过冗余凸点连接确保 D2W (die to wafer) 键合时最大限度提高键合良率。文献[55]提出了一种表面张力自组装的工艺,用于实现芯粒在晶圆基板上的自动键合。文献[56]采用冗余芯粒和冗余铜柱的方式提高系统良率。

上述学术研究试图通过工艺优化提高工艺生产过程的鲁棒性,这对保障 SoW 的鲁棒性具有重要的作用。实际上,这些由不确定物理失效导致的功能故障与由安全攻击导致的功能故障往往难以区分。例如,热效应导致的失效问题,可通过嵌入的热硬件木马触发;DoS 攻击导致的系统瘫痪和 TSV 物理故障导致的系统致瘫是一致的。因此,SoW 工艺鲁棒控制技术在一定程度上可以缓解 GSS 问题。

工艺优化尽管可以提升可靠性,但是难以解决由硬件安全攻击导致的功能安全问题。单独依赖工艺优化难以实现 SoW 系统的整体鲁棒性。假设 SoW 集成了 200 个 KGD 的芯粒,每个芯粒的微凸点数量为 1 000,若 D2W 贴装时,每个凸点的拼装良率为 99.99%,则整体晶圆的拼装良率约为 2.06×10^{-9} ,几乎为 0,即使将每个芯粒集成的良率提升为 99%,晶上系统的键合良率也仅有 13.4%。此外,正如文献[50]所指出的,SoW 的不确定物理失效问题主要表现在接口上,且失效场景不仅仅出现在系统使用前,更多地出现在系统使用中,这种系统使用中失效带来的影响更大,也更难解决。因此,针对互连接口的结构攻击一定是安全攻击的首选,因为攻击者认为安全攻击淹没在不确定物理失效中难以被察觉。反过来,对于防御者而言,解决物理失效问题的同时恰好可一体化解决 GSS 问题,这为安全策略高效部署提供了思路。从单纯工艺优化对 SoW GSS 的有限改善和运行时 SoW 更突出的 GSS 问题现状来看,需要进一步研究 SoW 的系统级鲁棒控制技术。

3.2 SoW 系统级鲁棒控制技术

结合 SoW 鲁棒性问题及物理失效的特点,

围绕 SoW 的系统级鲁棒控制技术研究主要集中在工艺系统级安全防御和晶上互连网络系统级安全架构上。

围绕 SoW 工艺系统级安全防御的研究,学术界和工业界可以直接参考的是 Tesla 所采用的软件重新规划路由方式,但是 DOJO 建立在硬件网络拓扑简单、软件调度管理简便的前提下,采用路径重规划实现故障芯粒的规避或绕行。文献[56]针对时钟网络传递过程中的安全问题,通过在物理位置上排布冗余的时钟接口,确保某一侧时钟接口故障后,其余接口的时钟依然可以传递进去。这种处理方式对于布局相同芯粒的 SoW 十分有效,因为相同芯粒的结构一致,可以确保芯粒四周的冗余接口保持物理位置的匹配,实现高效对接。但这限制了 SoW 异质异构芯粒的集成,对应的解决方法是设计归一化的芯粒间互连接口 IP 或者设计独立的互连芯粒。对于前者,现有的研究工作主要集中在 Chiplet 接口 IP 的冗余通道设计上,文献[57]的 UCle (universal chiplet interconnect express) 接口标准中每 32 bit 数据设置 2 bit 的冗余凸点用于规避集成过程的失效。文献[58]提出一种高速串行接口冗余通道设置方式,当发生故障时,可切换到冗余通道。文献[59]提出一种特制的互连芯粒结构,其中设计有故障检测电路,该电路能够通过发送特定序列检测连通性。但是该芯粒在晶圆级拼装的过程中需要先测试网络的连通性,在测试完成后再经过冗余的设计进行规避,并将故障信息广播至晶圆上的互连芯粒,以便调整路由。这种方式在应用前检测,规避效果很好,但是并不能很好地解决运行时的故障,且其需要先测试网络再进行其他功能芯粒的键合,功能芯粒的故障依然难以规避。

SoW 晶上互连网络系统级安全架构的研究工作主要集中在故障芯粒或者故障路径信息的检测、记录和规避方面。SoW 晶上互连网络多采用简单的 2D-Mesh 网络,网络维护简单。但实际上,SoW 晶上互连网络可以很复杂。目前针对 SoW 通用互连网络的容错研究并不多,考虑到网络的普适性,前文所述针对 IC 的 NoC 及 3D 互连网络的安全问题研究可作为 SoW 晶上

互连网络系统级安全架构研究的参考。针对网络的逻辑攻击问题, 现有的安全防御技术研究工作主要围绕网络重布局 (如网络拓扑的优化^[60-62]) 和路径重规划 (如自适应路由算法的设计^[63-66]) 展开, 试图通过提升动态性来解决安全问题。但围绕IC展开的算法革新归根结底受整个网络的路由节点及互连网络资源的限制, 使得只能在现有网络的基础上进行路径寻优。这对IC而言能够起到合理利用资源、最大化发挥系统功能的作用, 但对SoW而言并不一定是最优方法 (由于路由逻辑复杂、资源开销大、物理实现困难等综合原因, 在低拥塞的情况下开销较大, 还存在死锁问题, 应对攻击所采用的算法会带来资源的较大浪费)。然而实际上, 如果资源足够, 针对网络的逻辑攻击防御可以更灵活, 且可与功能处理本身融合, 以减小额外的资源开销。如图7所示, SoW具有极大的网络和极小的节点, 由晶圆级互连、多维网络、多互连模态等构建的晶上互连网络具有非常多的互连资源, 能够实现更加灵活的网络拓扑、更简单的路径寻优算法和更优的系统级鲁棒控制架构, 结合SoW GSS威胁模型可以进行一体化的广义鲁棒控制架构设计。

4 SoW GSS 技术发展趋势

目前学术界和产业界围绕SoW的研究仍停留在工艺技术和架构技术方面, 针对SoW GSS技术的研究较少 (现有的研究工作主要围绕SoW制备过程中软硬件的不确定物理失效展开)。但是从当前IC安全问题研究的现状和异构集成系统的发展趋势来看, SoW作为未来信息系统基础设施的新技术物理形态, 其GSS技术研究意义重大。尽管围绕SoW GSS技术的研究尚不充分, 但SoW GSS问题和广义鲁棒控制技术必然会成为未来SoW的主要研究方向之一。现有围绕IC的安全方法与技术, 以及网络空间内生安全技术都可作为SoW GSS技术的参考。

从传统IC的安全防御策略可以看出, 对不确定物理失效等随机触发的功能安全问题的防御已经研究出不少有效的解决方案, 其中增加系统或算法的动态、异构和冗余特性等的解决方案具有良好的效果。尽管这些解决方案存在不足, 但

SoW具有资源丰富、冗余、异构和动态等天然特性, 可以参考借鉴甚至弥补不足。其中, 文献[41]通过冗余芯粒保护硬件信息。文献[40]通过物理上的模糊设计规避木马的插入和故障触发, 可在SoW上通过架构优化解决冗余资源带来的面积开销。SoW同样可以基于文献[35]和文献[43]等在3D垂直互连NoC上构建安全策略的方法, 在假设晶圆基板上3D网络同样不可信的基础上, 构建安全策略; 文献[39]和文献[40]通过在系统中专门构建安全策略的方式和类似文献[42]所述的软硬件结合的安全策略更适用于本质上就部署有软硬件协同应用的SoW。

从最新的网络空间内生安全技术可以看出, 网络空间内生安全问题^[8,67-68]与其本征功能实体间是事物内部之间互相依赖又互相排斥的矛盾表达, 具有不可分割性, 只可能演进转化而不可能彻底消除。而SoW的GSS问题, 本质上是异构资源不可信及工艺不可靠和SoW应用服务的高动态特性两者之间互相依赖又互相排斥导致的, 因此网络空间内生安全问题的描述与SoW GSS威胁模型中功能安全、信息安全与网络安全的融合交织是一致的, 可以说SoW的GSS威胁模型是SoW网络空间内生安全的一种形象化表达。根据网络空间内生安全理论, 动态异构冗余 (dynamic heterogeneous redundancy, DHR)^[10,69]构造是一种动态异构冗余等价体的结构, 建立在“相对正确公理”逻辑表达与闭环鲁棒控制基础上, 基于策略裁决的迭代式多维动态重构结构, 由功能等价的异构执行体、输入/输出代理、采用迭代机制的策略裁决和反馈控制、调度器等构成, 可以一体化解决网络空间信息系统中功能安全和网络安全交织区中的内生安全共性问题。因此可以依托SoW在资源和架构上的优势, 在不额外增加系统开销的前提下, 将网络空间内生安全理论与SoW结合构建面向SoW GSS问题的DHR构造, 实现广义鲁棒控制。

SoW融合了工艺与结构的双重创新, 但单纯依赖工艺优化并不能显著提升系统级鲁棒性, 因此未来SoW GSS技术将主要围绕系统级广义鲁棒控制技术和SoW内生安全架构技术发展。

4.1 SoW GSS 一体化评价与测试

现有围绕 IC 安全问题的评价往往单一侧重功能安全或者信息安全, 这导致安全策略的制定通常采用“封门补漏”方式。随着测试难度的提升, SoW 融合交织在一起的 GSS 问题很难进行安全评价(无法区分安全问题的来源和判定安全策略是否可行), 因此未来 SoW GSS 的一体化评价与测试技术会成为研究的重点。

1) 针对 SoW 在宏观和微观层面设计过程中对模型类型、模拟精确度、仿真规模等维度提出的系统级仿真需求, 探索基础模型库建模维度与仿真层次、安全策略及安全评价模型抽象等关键技术。

2) 以 SoW 上非同源异构 DHR 中的“黑盒零部件”为基础模型, 通过相同应用部署下感知的“未知差模扰动”, 研究安全问题的精确定位和精准定性。

4.2 晶上互连网络动态异构冗余系统安全技术

SoW 典型的网络互连结构和归一化的接口特性, 使得围绕网络和接口的网络安全攻击成为威胁 GSS 安全的重点。但由于不确定物理失效问题需要灵活可靠的 NoW, 且网络安全攻击更容易淹没在不确定物理失效中, 因此系统级容错技术有望在最小开销下一体化解决 SoW 的 GSS 问题。传统的网络容错方法主要是基于网络的异构特性研究如何高效进行网络拓扑重构, 且受限于存储资源或者路由节点, 传统的网络容错大多围绕最优路径选择算法展开研究。而实际上, 两点之间的最优路径一定是有限约束下的直达路径。采用传统的最优路径选择算法和网络拓扑重构方法会导致收敛速度很慢, 但是 SoW 丰富的节点资源和互连资源为直达路径的构建提供了可行性。

1) 研究基于多维归一化网络的系统容错路径规划, 包括通过构建数据和电路共存的节点结构和多维层面的归一化网络设计实现 SoW 的多维网络架构设计。

2) 研究接口级的动态异构冗余容错技术和系统级网络拓扑优化技术, 如归一化网络下的直达路径规划和基于交通博弈的网络拓扑优化的系统容错技术。

4.3 基于 DHR 构造的 SoW 广义鲁棒控制架构

非 SoW 内生安全的研究主要基于 DHR 构造, 而 DHR 构造要求冗余等价体最大限度异构, 且需要同步处理异构冗余等价体的策略裁决。策略裁决的同步约束使得 SoW 的安全架构和系统性能需要协同考虑, 异构执行体的物理布局很容易因无约束优化带来设计空间探索的无解。此外, SoW 规模极大, 策略裁决对调度的实时性和同步要求更高。基于 DHR 构造的 SoW 广义鲁棒控制架构可围绕 SoW 异构冗余等价体最优布局 and SoW DHR 构造下的高效策略调度进行研究。

1) 通过构建图约束的因果结构和基于图网络的描述方法将系统架构探索简化为有限约束下的设计空间探索。将异构执行体无约束优化转化为有限约束下的优化, 从而加速收敛。

2) 采用分布式的多级调度和裁决机制在局部和全局实现实时和同步调度。考虑到晶圆上众多的异构资源, 不可能在整个晶圆上完成异构冗余等价体的构建和判决, 因此采用分区域设置方式, 在区域内部进行 DHR 构造, 不同区域之间进行分布式的多级调度和裁决。

5 结束语

SoW 是集成电路工艺集成微系统结构和复杂应用宏系统架构的总和, 不仅具有工艺不确定物理失效导致的功能安全问题, 还兼有针对集成电路逻辑攻击导致的信息安全问题和针对系统应用攻击导致的网络安全问题, 三者构成 SoW 复杂的 GSS 问题。本文从集成电路 IC 和异构集成电路的安全问题出发, 对 SoW GSS 问题的产生、研究挑战和研究意义进行阐述, 提出首个 SoW GSS 威胁模型, 并提出将 SoW 架构与网络空间内生安全技术结合研究的思路, 探索 SoW GSS 问题的解决方法。此外, 对 SoW 鲁棒控制技术的研究现状进行了分析, 得出工艺鲁棒控制和系统级鲁棒控制技术存在的不足, 进而分析了一体化解决 SoW GSS 问题的可行性, 最后给出了 SoW GSS 技术与网络空间内生安全技术融合下的发展趋势, 为 SoW 的安全问题研究提供理论指导和发展方向参考。

参考文献:

- [1] 吴林晟, 毛军发. 从集成电路到集成系统[J]. 中国科学: 信息科学, 2023, 53(10): 1843-1857.
WU L S, MAO J F. From integrated circuits to integrated systems [J]. Science in China(Information Sciences), 2023, 53(10): 1843-1857.
- [2] 郭江兴, 刘勤让, 沈剑良, 等. 从SoC到SDSoW: 微电子发展的新范式[J]. 中国科学: 信息科学, 2024, 54(6): 1350-1368.
WU J L, LIU Q R, SHEN J L, et al. From SoC to SDSoW: a new paradigm for microelectronics development[J]. Science in China(Information Sciences), 2024, 54(6): 1350-1368.
- [3] FIEVREA A, AL-AKHIR A, BHANSALIA S. Integrated circuit security: an overview[J]. Journal of the Institute of Smart Structures and Systems, 2015, 4(1): 18-37.
- [4] ABRAMOVICI M, BRADLEY P. Integrated circuit security: new threats and solutions[C]//Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies. 2009: 1-3.
- [5] NABEEL M, ASHRAF M, PATNAIK S, et al. 2.5D root of trust: secure system-level integration of untrusted chiplets[J]. IEEE Transactions on Computers, 2020, 69(11): 1611-1625.
- [6] KNECHTEL J, PATNAIK S, SINANOGLU O. 3D integration: another dimension toward hardware security[C]//Proceedings of 2019 IEEE 25th International Symposium on on-Line Testing and Robust System Design (IOLTS). Piscataway: IEEE Press, 2019: 147-150.
- [7] KHAN M S M, XI C, KHAN A A, et al. Secure interposer-based heterogeneous integration[J]. IEEE Design & Test, 2022, 39(6): 156-164.
- [8] 郭江兴. 论网络空间内生安全问题及对策[J]. 中国科学: 信息科学, 2022, 52(10): 1929-1937.
WU J X. Cyberspace's endogenous safety and security problem and the countermeasures[J]. Science in China(Information Sciences), 2022, 52(10): 1929-1937.
- [9] 郭江兴. 工业控制网络广义功能安全问题与解决之道[J]. 信息安全研究, 2022, 8(6): 524-527.
WU J X. Generalized functional safety problems and solutions in industry control network [J]. Journal of Information Security Research, 2022, 8(6): 524-527.
- [10] 郭江兴. 网络空间内生安全—拟态防御与广义鲁棒控制[M]. 北京: 科学出版社, 2020.
WU J X. Principle of cyberspace mimic defense-generalized robust control and endogenous security[M]. Beijing: Science Press, 2020.
- [11] ANDERSON R, KUHN M. Low cost attacks on tamper resistant devices[C]//Proceedings of International Workshop on Security Protocols. Berlin: Springer, 1997: 125-136.
- [12] TSANG Y L, NALLAPATI G, Skarupa R, et al. Identification of extension implant defect in sub-micron CMOS ICs-analysis technique, model, and solution[C]//Proceedings of International Symposium for Testing and Failure Analysis. 2011, 38268: 212-217.
- [13] TORRANCE R, JAMES D. The state-of-the-art in semiconductor reverse engineering[C]//Proceedings of the 48th Design Automation Conference. 2011: 333-338.
- [14] ALASAD J S P. Strong logic obfuscation with low overhead against IC reverse engineering attacks[J]. ACM Transactions on Design Automation of Electronic Systems. New York: ACM Press, 2020, 25(4): 1-31.
- [15] PATNAIK S, ASHRAF M, SINANOGLU O, et al. Obfuscating the interconnects: low-cost and resilient full-chip layout camouflaging[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39(12): 4466-4481.
- [16] AMINI E, HERFURTH N, BEYREUTHER A, et al. Generation and tracking of optical signals inside the IC to improve device security and failure analysis[C]//Proceedings of 2019 IEEE 26th International Symposium on Physical and Failure Analysis of Integrated Circuits (IPFA). Piscataway: IEEE Press, 2019: 1-6.
- [17] XI C, KHAN A A, RAHMAN M T, et al. Security assessment of IC packaging against optical attacks[J]. EDFA Technical Articles, 2021, 23(2): 4-12.
- [18] SKOROBOGATOV S P. Semi-invasive attacks – a new approach to hardware security analysis[R]. University of Cambridge, Computer Laboratory, 2005.
- [19] WANG H, LI H, RAHMAN F, et al. SoFI: security property-driven vulnerability assessments of ICs against fault-injection attacks[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021, 41(3): 452-465.
- [20] FADIHEH M R, WEZEL A, MUELLER J, et al. An exhaustive approach to detecting transient execution side channels in RTL designs of processors[J]. IEEE Transactions on Computers, 2022, 72(1): 222-235.
- [21] ZHANG L, VEGA L, TAYLOR M. Power side channels in security ICs: hardware countermeasures[J]. arXiv preprint, arXiv: 1605.00681, 2016.
- [22] WANG F Z, WANG Q J, FU B Q, et al. Security closure of IC layouts against hardware trojans[C]//Proceedings of the 2023 International Symposium on Physical Design. New York: ACM Press, 2023: 229-237.
- [23] QU G. Hardware security and trust: a new battlefield of information[C]//Proceedings of Decision and Game Theory for Security: 11th International Conference. 2020: 486-501.
- [24] SKOROBOGATOV S, WOODS C. Breakthrough silicon scanning discovers backdoor in military chip[C]//Proceedings of 14th International Workshop on Cryptographic Hardware and Embedded Systems – CHES 2012. Berlin: Springer, 2012: 23-40.
- [25] HUANG Y, MISHRA P, FARAHMANDI F. System-on-chip security: validation and verification[M]. Berlin: Springer, 2020.
- [26] CHARLES S, MISHRA P. A survey of network-on-chip security attacks and countermeasures[J]. ACM Computing Surveys(CSUR), 2021, 54(5): 1-36.
- [27] SUDUSINGHE C, CHARLES S, AHANGAMA S, et al. Eavesdropping attack detection using machine learning in network-on-chip architectures[C]//Proceedings of 16th IEEE International Symposium on Networks-on-Chip (NOCs). 2022: 21-28.
- [28] CHARLES S, MISHRA P. Lightweight and trust-aware routing in NoC-based SoCs[C]//Proceedings of 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). 2020: 160-167.

- [29] CHARLES S, LYU Y, MISHRA P. Real-time detection and localization of distributed DoS attacks in NoC-based SoCs[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2020, 39(12): 4510-4523.
- [30] HAAS G, POTLURI S, AYSU A. ITimed: cache attacks on the apple a10 fusion SoC[C]// *Proceedings of 2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. Piscataway:IEEE Press, 2021: 80-90.
- [31] MAILLARD J, HISCOCK T, LECOMTE M, et al. Side-channel disassembly on a system-on-chip: a practical feasibility study[J]. *Microprocessors and Microsystems*, 2023, 101: 104904.
- [32] LI T, HOU J, YAN J, et al. Chiplet heterogeneous integration technology-status and challenges[J]. *Electronics*, 2020, 9(4): 670-681.
- [33] SHEIKH F, NAGISETTY R, KARNIK T, et al. 2.5D and 3D heterogeneous integration: emerging applications[J]. *IEEE Solid-State Circuits Magazine*, 2021, 13(4):77-87.
- [34] RAO V V, SASAN A, SAVIDIS I. Analysis of the security vulnerabilities of 2.5-D and 3-D integrated circuits[C]//*Proceedings of the 23rd International Symposium on Quality Electronic Design (ISQED)*. Piscataway:IEEE Press, 2022: 1-7.
- [35] DOFE J, YU Q, WANG H, et al. Hardware security threats and potential countermeasures in emerging 3D ICs[C]//*Proceedings of the 26th Great Lakes Symposium on VLSI*. New York: ACM Press, 2016: 69-74.
- [36] DOFE J, GU P, STOW D, et al. Security threats and countermeasures in three-dimensional integrated circuits[C]//*Proceedings of the on Great Lakes Symposium on VLSI 2017*. New York: ACM Press, 2017: 321-326.
- [37] MOEIN S, GULLIVER T A, GEBALI F, et al. A new characterization of hardware trojans[J]. *IEEE Access*, 2016,4:2721-2731.
- [38] ZHANG Z, YU Q. Modeling hardware trojans in 3D ICs[C]//*Proceedings of 2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. Piscataway:IEEE Press, 2019: 483-488.
- [39] VALAMEHR J, SHERWOOD T, KASTNER R, et al. A 3-D split manufacturing approach to trustworthy system development[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2013,32(4):611-615.
- [40] PATNAIK S, ASHRAF M, SINANOGLU O, et al. A modern approach to IP protection and trojan prevention: split manufacturing for 3D ICs and obfuscation of vertical interconnects[J]. *IEEE Transactions on Emerging Topics in Computing*, 2019, 9(4): 1815-1834.
- [41] SHAYAN M, BASU K, KARRI R. Security assessment of interposer-based chiplet integration[J]. *arXiv preprint arXiv: 2010.13155*, 2020.
- [42] HASAN M, CRUZ J, CHAKRABORTY P, et al. Trojan resilient computing in cots processors under zero trust[J]. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2022, 30(10): 1412-1424.
- [43] ZHANG Z, YU Q. Invariance checking based Trojan detection method for three-dimensional integrated circuits[C]//*Proceedings of 2020 IEEE International Symposium on Circuits and Systems (ISCAS)*. Piscataway:IEEE Press, 2020: 1-5.
- [44] JANGAM S C, IYER S S. Silicon-interconnect fabric for fine-pitch ($\leq 10\mu\text{m}$) heterogeneous integration[J]. *IEEE Transactions on Components, Packaging and Manufacturing Technology*, 2021, 11(5): 727-738.
- [45] LI S. SiP system-in-package design and simulation: mentor EE flow advanced design guide[M]. Hoboken: John Wiley & Sons, 2017.
- [46] PAL S, PETRISKO D, TOMEI M, et al. Architecting waferscale processors-a GPU case study[C]//*Proceedings of 2019 IEEE International Symposium on High Performance Computer Architecture (HPCA)*. Piscataway:IEEE Press, 2019: 250-263.
- [47] MÖLLER D P F. Guide to cybersecurity in digital transformation: trends, methods, technologies, applications and best practices[M]. Berlin:Springer Nature, 2023.
- [48] LAUTERBACH G. The path to successful wafer-scale integration: the Cerebras story[J]. *IEEE Micro*, 2021, 41(6): 52-57.
- [49] TALPES E, WILLIAMS D, SARMA D D. DOJO: the microarchitecture of tesla's exa-scale computer[C]//*Proceedings of 2022 IEEE Hot Chips 34 Symposium (HCS)*. Piscataway: IEEE Press, 2022: 1-28.
- [50] CHASE N S, IRWIN R, YANG Y T, et al. Reliability considerations for wafer scale systems[C]// *Proceedings of 2021 IEEE 71st Electronic Components and Technology Conference (ECTC)*. Piscataway:IEEE Press, 2021: 84-89.
- [51] IYER S S, BAJWA A A. Reliability challenges in advance packaging[C]// *Proceedings of 2018 IEEE International Reliability Physics Symposium (IRPS)*. Piscataway:IEEE Press, 2018.
- [52] WAN Z, WINSTEL K, KUMAR A, et al. Low-temperature wafer bonding for three-dimensional wafer-scale integration[C]//*Proceedings of 2018 IEEE SOI-3D-Subthreshold Microelectronics Technology Unified Conference (S3S)*. Piscataway:IEEE Press, 2018: 1-2.
- [53] GOORSKY M S, SCHJOLBERG-HENRIKSEN K, BEEKLEY B, et al. Low temperature metal-metal bonding for heterogeneous integration and performance scaling[C]//*Proceedings of the 5th International Workshop on Low Temperature Bonding for 3D Integration (LTB-3D)*. Piscataway:IEEE Press, 2017.
- [54] PAL S, ALAM I, SAHOO K, et al. I/O architecture, substrate design, and bonding process for a heterogeneous dielet-assembly based waferscale processor[C]//*Proceeding of 2021 IEEE 71st Electronic Components and Technology Conference (ECTC)*. Piscataway:IEEE Press, 2021: 298-303.
- [55] FUKUSHIMA T, IWATA E, LEE K W, et al. Self-assembly technology for reconfigured wafer-to-wafer 3D integration[C]//*Proceedings of 2010 Proceedings 60th Electronic Components and Technology Conference (ECTC)*. Piscataway:IEEE Press, 2010: 1050-1055.
- [56] PAL S, LIU J, ALAM I, et al. Designing a 2048-chiplet, 14336-core waferscale processor[C]//*Proceedings of 2021 58th ACM/IEEE Design Automation Conference (DAC)*. Piscataway:IEEE Press, 2021: 1183-1188.
- [57] SHARMA D D, PASDAST G, QIAN Z, et al. Universal chiplet interconnect express (UCIe): an open industry standard for innovations with chiplets at package level[J]. *IEEE Transactions on Components, Packaging and Manufacturing Technology*, 2022, 12(9): 1423-1431.

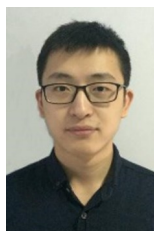
- [58] SUNDARAM J, GOPAL S, THOMAS T P, et al. A reconfigurable asynchronous SERDES for heterogenous chiplet interconnects[C]// Proceedings of 2021 22nd International Symposium on Quality Electronic Design (ISQED). Piscataway: IEEE Press, 2021: 542-546.
- [59] VAISBAND B, BAJWA A, IYER S S. Network on interconnect fabric[C]// Proceedings of 2018 19th International Symposium on Quality Electronic Design (ISQED). Piscataway: IEEE Press, 2018: 138-143.
- [60] DALLY W J, TOWLES B. Route packets, not wires: on-chip interconnection networks[C]// Proceedings of the 38th Annual Design Automation Conference. New York: ACM Press, 2001: 684-689.
- [61] BENINI L, MICHELI G D. Networks on chips: a new SoC paradigm[J]. Computer, 2002, 35(1): 70-78.
- [62] LIU C C, CHEN J H, MANOHAR R, et al. Mapping system-on-chip designs from 2-D to 3-D ICs[C]// Proceedings of 2005 IEEE International Symposium on Circuits and Systems (ISCAS). Piscataway: IEEE Press, 2005: 2939-2942.
- [63] YING H Y, HOFMANN K, HOLLSTEIN T. Dynamic quadrant partitioning adaptive routing algorithm for irregular reduced vertical link density topology 3-dimensional network-on-chips[C]// Proceedings of 2014 International Conference on High Performance Computing & Simulation (HPCS). Piscataway: IEEE Press, 2014: 516-522.
- [64] CHANG W C, TSENG H W, KUO C F. A traffic-balanced routing scheme for heat balance in 3D networks-on-chip[C]// Proceedings of the 29th Annual ACM Symposium on Applied Computing. New York: ACM Press, 2014: 1437-1442.
- [65] KUMAR M, LAXMI V, GAUR M, et al. Highly adaptive and congestion-aware routing for 3D NoCs[C]// Proceedings of the 24th Edition of the Great Lakes Symposium on VLSI. New York: ACM Press, 2014: 97-98.
- [66] AHMED A B, ABDALLAH A B. Graceful deadlock-free fault-tolerant routing algorithm for 3D network-on-chip architectures[J]. Journal of Parallel and Distributed Computing, 2014, 74(4): 2229-2240.
- [67] 邬江兴. 网络空间内生安全发展范式[J]. 中国科学: 信息科学, 2022, 52(2): 189-204.
- WU J X. Development paradigms of cyberspace endogenous safety and security[J]. Science in China(Information Sciences), 2022, 52(2): 189-204.
- [68] WU J X. Cyberspace mimic defense[M]. Cham: Springer International Publishing, 2020.
- [69] 邬江兴. 内生安全赋能网络弹性工程[M]. 北京: 科学出版社, 2023.

WU J X. Endogenous safety and security empowers cyber resilience engineering [M]. Beijing: Science Press, 2023.

[作者简介]



李沛杰 (1990-), 男, 山西襄汾人, 信息工程大学助理研究员, 主要研究方向为软件定义晶上系统、硬件安全、软件定义互连。



郭威 (1990-), 男, 北京人, 信息工程大学副教授, 主要研究方向为计算机体系结构、人工智能与大数据、内生安全。



沈剑良 (1982-), 男, 浙江德清人, 信息工程大学教授, 主要研究方向为片上系统芯片、软件定义晶上系统。



曹志鹏 (1996-), 男, 陕西西安人, 信息工程大学博士生, 主要研究方向为软件定义晶上系统、计算机体系结构、互连网络。



梅波 (1998-), 男, 安徽宣城人, 信息工程大学博士生, 主要研究方向为内生安全、硬件木马防御。