NEUROPULS：基于相变材料增强硅光子学的神经形态高能效安全加速器

Fabio Pavanello[1], Cedric Marchand[1], Ian O'Connor[1],R´egis Orobtchouk[1],Fabien Mandorlo[1],Xavier Letartre[1],Sebastien Cueff[1], Elena Ioana Vatajelu[2], Giorgio Di Natale[2],Benot Cluzel[3],Aurelien Coillet[3],Benoit Charbonnier[4],Pierre No´e[4], Frantisek Kavan[5], Martin Zoldak[5],Michal Szaj[5],Peter Bienstman[6],Thomas Van Vaerenbergh[7],Ulrich Ruhrmair[8], Paulo Flores[9], Luis Guerra e Silva[9],Ricardo Chaves[9],Luis-Miguel Silveira[9],Mariano Ceccato[10],Dimitris Gizopoulos[11], George Papadimitriou[11], Vasileios Karakostas[11],Axel Brando[12],Francisco J. Cazorla[12],Ramon Canal[12,13], Pau Closas[14], Adri´a Gusi-Amig´o[14],Paolo Crovetti[15],Alessio Carpegna[16],Tzamn Melendez Carmona[16],Stefano Di Carlo[16],Alessandro Savino[16]

[1]里昂大学、里昂中央理工学院、里昂国立应用科学学院、里昂第一克洛德·贝尔纳大学、里昂高等化学物理电子学院、法国国家科学研究中心、INL[2]格勒诺布尔阿尔卑斯大学、法国国家科学研究中心、格勒诺布尔国立理工学院、TIMA，法国格勒诺布尔38000[3]ICB CNRS第6303联合研究单位、勃艮第-弗朗什-孔泰大学、法国第戎[4]格勒诺布尔阿尔卑斯大学、法国原子能和替代能源委员会、LETI，法国格勒诺布尔， [5]ARGOTECH，捷克纳霍德[6]根特大学 - imec，比利时根特， [7]惠普实验室、HPE Belgium，比利时迪赫姆B-1831[8]慕尼黑大学物理系，德国慕尼黑， [9]里斯本 INESC-ID，葡萄牙里斯本[10]计算机科学系，维罗纳大学–意大利维罗纳[11]信息学与电信系，雅典国立卡波季斯特里亚大学，希腊雅典[12]巴塞罗那超级计算中心，西班牙巴塞罗那， [13]加泰罗尼亚理工大学，西班牙巴塞罗那[14]Albora Technologies SL，西班牙巴塞罗那[15]都灵理工大学，电子与电信系（DET），意大利[16]都灵理工大学，控制与计算机工程系，意大利

arXiv:2305.03139v1 [cs.AR] 4 May 2023

摘要—**本文介绍"地平线欧洲"计划下的 NEUROPULS 项目，该项目致力于利用增强型硅光子技术，开发安全、高能效且采用 RISC-V 接口的神经形态加速器。我们旨在开发增强型硅光子平台、由 FPGA 驱动并连接 RISC-V 的计算平台，以及完整的仿真平台，以展示神经形态加速器的能力。具体而言，我们将讨论各平台底层技术的主要优势与局限。随后，我们将探讨面向边缘计算应用的三种目标用例：全球卫星导航系统（GNSS）抗干扰、自动驾驶，以及边缘设备中的异常检测。最后，我们将讨论独立式加速器实现及项目用例的可靠性与安全性问题。**

索引词—**人工神经网络、建模、仿真**

I. 引言

处理大量数据的需求日益增长，这已成为开发新型高能效计算架构 [1]的主要驱动力。在众多满足能效要求的方法中，受大脑启发的神经形态架构是最可行的解决方案之一，这得益于其存储器与处理单元之间天然不存在输入/输出瓶颈，并且能够更自然地映射机器学习（ML）算法 [2]。神经形态方法尤其适用于开发轻量、低延迟、低功耗的加速器，满足边缘计算系统在自动驾驶、物联网（IoT）设备和 5G网络等应用中的需求。

在构建神经形态架构的各种技术中，光子集成能够高效满足上述所有需求 [3]这主要得益于目前成熟的CMOS兼容平台已可供使用，例如绝缘体上硅（SOI），它们支持密集集成调制器、探测器、光学接口等器件，以实现规模扩展。具体而言，与电子技术相比，光子学方法在能耗、带宽和延迟方面具有关键优势，这得益于光子集成电路（光子集成电路）中的低传播损耗，以及通过波分复用技术、高速数据编码/解码器件和光子内部的光速传播实现大规模并行的可能性

本项目获得欧盟"地平线欧洲"研究与创新计划资助，资助协议编号为 101070238。本文所表达的观点和意见仅代表作者本人，并不一定反映欧盟的立场。欧盟及其资助机构均不对这些观点和意见承担责任。

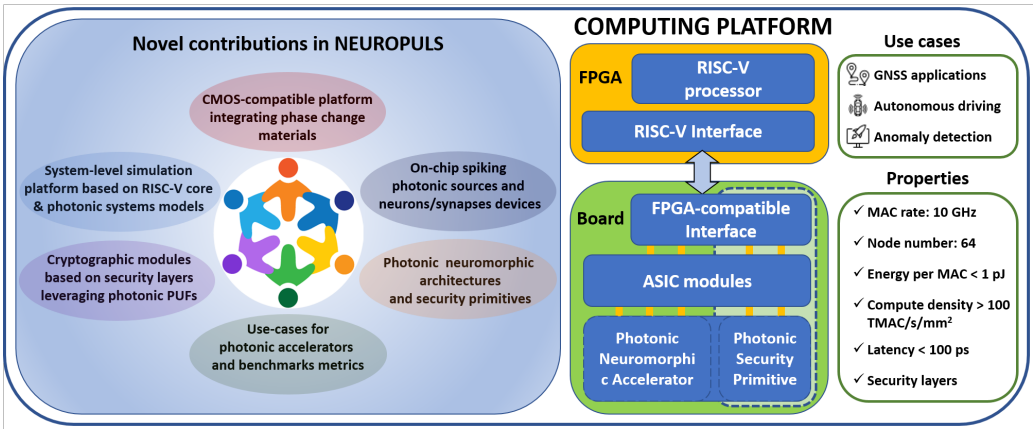

图 1. NEUROPULS 项目带来的创新贡献概览（左侧），以及将开发的计算平台、预期性能和目标应用场景（右侧）。

组件 [4]。

下文将概述 NEUROPULS 项目及其科学目标，介绍该项目如何增强欧洲数字供应链，并开发欧洲安全专用加速器设计，使其能够以超低功耗运行实现高性能计算。NEUROPULS 的独特技术将使目标边缘应用的每瓦性能至少提升两个数量级，从而解决当前基于 CMOS 的通用计算平台性能下降以及摩尔定律放缓的问题。

II. NEUROPULS 中提出的方法

在 NEUROPULS 中，我们将在技术、硬件计算和仿真层面开发三个不同的平台（见图 1）。技术平台基于法国原子能和替代能源委员会-LETI 的开放式硅光子平台，并加入相变材料（相变材料）和 III-V 材料。基于这些技术构建的模块，例如可塑性非易失光子突触 [5] 和基于脉冲激光器 [6]，的非线性神经元，将支持 NEUROPULS 探究各种神经形态光子架构。

安全层将基于物理不可克隆函数（PUF）构建，这类安全原语无需将数字密钥存储在存储器中 [7]。这些原语将嵌入光子芯片和电子芯片中。软硬件接口将利用硅级安全层，为加速器设置多种安全功能，例如安全认证、神经网络（NN）数据加密以及输出数据签名。

通过高速射频布线与封装，光子架构将由与 PIC 芯片相连的 ASIC 芯片驱动。随后，开发出的加速器将连接到一块 FPGA，RISC-V 处理器将在其中实现。该处理器将作为外部世界与加速器之间的接口，用于传输和接收原始数据及计算结果，并处理安全协议，同时利用安全原语。按照我们的设想，ASIC 芯片还将集成 RISC-V 处理器，以便进行大规模制造，从而构建独立且自洽的硬件计算平台。不过，出于原型开发的考虑，NEUROPULS 中的 ASIC 将仅包含驱动电路、与 FPGA 的接口以及电子物理不可克隆函数。后者将用于确保硬件完整性，以独特方式绑定光子芯片和电子芯片。PIC 芯片和 ASIC 芯片将安装在电路板上，并通过 FPGA 接口连接到搭载 RISC-V 处理器的 FPGA。

我们还将针对基于相变材料的光子器件和系统，开发不同复杂度级别的计算模型，以仿真在硅光子平台上流片的神经形态架构和物理不可克隆函数架构的行为，以及将它们纳入整个计算平台后的响应。最后，我们将把加速器应用于边缘计算中的三个重要用例：GNSS 抗干扰、自动驾驶和边缘设备异常检测。考虑整个硬件计算平台的先进仿真工具，将使我们能够研究加速器的性能扩展，例如能耗、延迟和速度如何随输入/输出数量、层数、神经元数量等变化，以及其安全功能。在 NEUROPULS 中，我们的目标是让加速器实现极高的性能；对于所选的边缘计算用例，这将使我们能够将能量/MAC 指标提升例如两个数量级，优于同类 GPU 技术。此外，我们将针对独立式加速器和目标用例，采用硬件和软件方法研究基于物理不可克隆函数的安全功能，涵盖从安全原语到软件驱动的安全协议实现。

III. CMOS兼容平台

项目中将开发的平台基于法国原子能和替代能源委员会（CEA）-LETI 的硅光子平台，可通过开放获取的多项目晶圆流片获得。该平台已经包含多个关键构建模块，例如光学接口（光栅耦合器）、调制器、探测器、谐振器等（见图 2）。

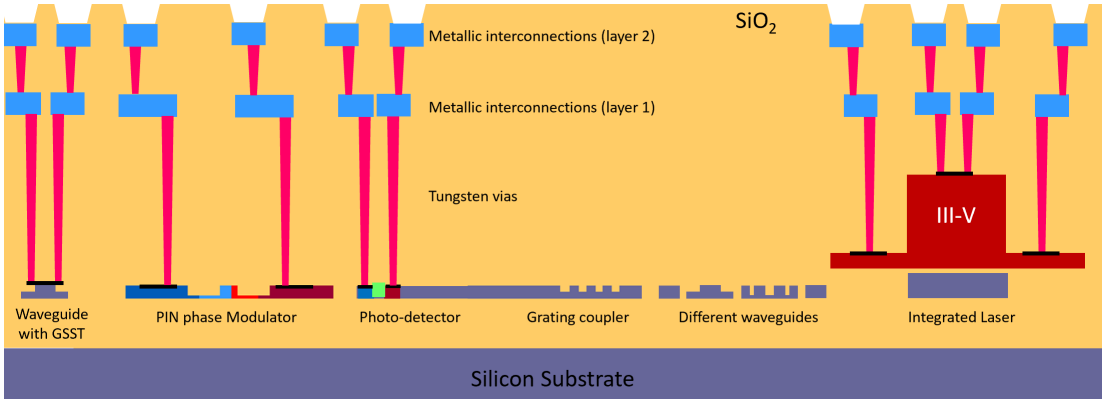

图 2. NEUROPULS 增强型硅光子平台的横截面。GSST 等相变材料（左侧）和 III-V 族材料（右侧）集成在波导顶部。平台提供两层互连线，用于布线。

然而，我们计划集成的一项创新功能包括相变材料（PCMs）。这些薄型相变材料层，例如具有不同化学计量组成的 GeSbTe（GST）和 GeSSbTe（GSST）材料，将以薄型（厚度为 10–20 nm）的矩形贴片形式放置在光学波导上方，如图 2 所示。由于相变材料状态不同（即非晶态与晶态）会导致有效折射率发生变化，其集成将影响光场传播。借助光场与相变材料贴片之间的相互作用，可以实现对光学特性的强力调制。平台将提供多种波导，即条形（完全刻蚀）和脊形（部分刻蚀）结构，其中硅层总厚度为 300 nm。平台还将配备两层金属互连层，以便于组件布线；此外还会包含加热器（未显示在截面图中），用于改变相变材料的结晶程度。得益于高性能行波调制器和锗探测器，该平台能够在 50 GHz 以上的频率下运行。

IV. 硬件计算平台

在光学架构方面，我们将实现多种方案，结合硅光子学与相变材料。

一种直接的方案是采用加速器，对前馈神经网络（FFNN）中的矩阵-向量乘积进行运算；通过对调制器网格进行编程，使系统实现特定的矩阵乘法 [4]。例如，可以使用奇异值分解，将矩阵分解为一个酉矩阵、一个对角矩阵和另一个酉矩阵的乘积。

这里的主要限制在于，光学元件的尺寸使得实现大型矩阵变得困难。因此，我们还将探索实现更大规模系统的其他方案。我们将考虑的一种方法是剪枝，即移除网络中不必要的连接和权重，以减小矩阵的整体规模。另一种方法是采用分块矩阵分解，将矩阵划分为可以分别处理的较小数据块。这样一来，就能用较少的光学元件实现更大的矩阵。

此外，我们还将探索 [8] 中提出的张量列车方法。这些方法将矩阵表示为多个低秩张量的乘积，从而能够利用光学元件更高效地进行处理。通过采用这些不同的方法，我们旨在开发一种可扩展的光学架构，以处理更大的矩阵和更复杂的神经网络。这将使基于光子学的神经网络训练更快速、更具可扩展性且更高效。除了前馈架构外，我们还将研究循环神经网络（RNN）。我们可以考虑完全可训练的 RNN，但也会考虑一种称为储备池计算的变体。在储备池计算中，RNN 经过随机初始化后不再训练，而是对各节点信号随时间变化的轨迹进行线性组合训练。这种技术的优势在于，与完全可训练的 RNN 相比，它的计算效率更高，同时在许多应用中仍能取得良好性能。此前，这种方法已在集成光子学中得到应用 [9]。例如，它已用于实现电信信号的非线性色散补偿 [10], , 展现了光子学在传统机器学习之外广泛应用领域中的潜力。

我们计划在所提出的架构中引入相变材料，以实现非易失性光学权重。多项研究已使用过这些材料，例如 [11] 和 [12]。与易失性权重相比，使用非易失性权重可显著降低功耗；易失性权重则必须持续驱动或定期刷新。不过，除了非易失性之外，相变材料还有另一项我们计划在架构中加以利用的优势：其非线性动力学。例如，通过脉冲而非连续波激励材料，我们可以利用材料的非线性行为来实现其他计算范式，例如脉冲神经网络（SNNs）。在此类神经网络中，神经元通过短暂的脉冲或尖峰而非连续变化的信号进行通信。这使得实现高能效、高度并行的神经网络成为可能。为了生成注入系统的尖峰，我们将在同一平台上单片集成 III-V 族材料激光器，开发高消光比（ER > 8 dB）的先进 Q 开关脉冲激光器 [13]。这些混合集成的 III-V 族材料硅基脉冲激光器是一种可扩展且低成本的替代方案，可替代

这些调 Q 激光器早期的纯 III-V 版本。

V. 仿真平台

新型硬件架构需要构建一个先进工具生态系统，以支持并推动创新的硬件方案。具体而言，要实现创新，就必须借助仿真工具，在探索新技术功能优势的同时，准确评估加速器对最终系统在性能、功耗和可靠性等方面的影响。

NEUROPULS 项目旨在开发一个仿真平台，用于建模和评估集成神经形态加速器与硬件安全原语的计算系统。该仿真平台将探索异构计算系统的设计空间，利用光子神经形态加速器和硬件原语实现最佳性能。项目将设计并实现一套用于系统级建模与仿真的工具链，使光子学加速器具备功能并可编程。该工具链将自动生成复杂度和精度各异的光子模块系统级模型。仿真平台将对完整的计算系统进行建模，包括多个 CPU 核心、存储器层级、PNN 和基于物理不可克隆函数（PUF）的光子安全原语。该平台还将涵盖计算堆栈的所有层，从硬件到应用软件。为评估光子技术的安全保障，仿真平台将考量系统层和应用软件层的所有软件安全方面。

该平台将以 gem5 [14], [15] 为基础：这是一款先进的微架构级模拟器，已广泛应用于多项研究 [14]–[16]。我们将通过近期扩展增强该模拟器，使其支持基于 RISC-V 的系统建模，并提供丰富的加速器和灵活的接口。平台的灵活性将有助于探索不同安全级别与相应的性能、功耗和可靠性代价之间的权衡。

NEUROPULS 还将研究光子硬件组件的可靠性和功耗估算。NEUROPULS 仿真平台旨在提供灵活的基础设施，以便比较各种光子加速器参数，从而确定神经形态硬件在降低功耗和提升性能方面的效果。此外，该平台将重点关注 RISC-V CPU 核心和定制神经形态加速器及其相应的软件栈，以评估完整异构系统的可靠性，并识别不同神经网络加速器可能面临的潜在可靠性问题。因此，NEUROPULS 将创建一个快速、灵活且模块化的仿真平台。该平台将以 gem5 仿真器为基础构建，并支持对先进神经网络加速器和物理不可克隆函数进行评估。

VI. 目标应用场景

A. GNSS 抗干扰

基于卫星的导航系统（称为 GNSS）为众多应用中的位置、速度和时间（PNT）估算提供了准确可靠的解决方案 [17]。然而，GNSS 可能受到 L 波段有意或无意的干扰，干扰通常会压制 GNSS 接收机，意图使其无法正常工作[18]。如今，干扰事件并不少见，干扰器既容易买到，也容易自制 [19],，这会威胁依赖 GNSS PNT 的安全关键型应用或关键基础设施。因此，干扰管理对于确保 GNSS 的弹性使用至关重要，其中包括检测并分类干扰事件。在此背景下，研究表明[20], [21] ，机器学习模型能够取得令人期待的结果，包括以分布式联邦学习方式训练这些模型的方案 [22]。NEUROPULS 致力于解决这一应用场景，通过支持高效的基于神经网络的分类器，向用户预警干扰的存在及其类型。

B. 自动驾驶

轨迹预测是阿波罗 [23] 和 Autoware [24] 等自动驾驶框架的基础。一些轨迹预测系统在不同程度上采用循环神经网络。例如，阿波罗将这类网络用于其轨迹预测系统。其他基于长短期记忆（LSTM）的实现则采用基于LSTM的多输入多输出循环神经网络 [25]。因此，高效的循环神经网络实现为自动驾驶系统中的轨迹预测带来了新的机遇。NEUROPULS 将利用其加速技术，探索基于循环神经网络的轨迹预测系统的效率。我们的目标是首先从阿波罗中较简单的循环神经网络部分入手，主要用于测试该方法的可行性，然后扩展至更复杂的基于长短期记忆的循环神经网络，以在轨迹预测应用场景中检验该方法的能力极限。

C. 边缘设备中的异常检测

作为 NEUROPULS 项目开发的光子神经形态加速器用于网内计算的一个示例，我们将面向安全应用，研究由光子硬件仿真的神经网络在资源受限的边缘环境中执行异常检测的潜力。将这些超高速神经形态加速器嵌入边缘端以标记异常，可帮助识别恶意事件；否则，这些事件就需要通过成本更高的后处理来识别。可能的应用场景包括防范物联网僵尸网络、分布式拒绝服务攻击 [26],[27], 或车载网络安全 [28]。异常检测本质上是事件驱动的。因此，它可能非常适合利用脉冲神经网络 [28], [29],实现的时间信息处理；脉冲神经网络是 NEUROPULS 项目研究的神经网络架构之一。首先，我们旨在利用项目开发的硬件模型和仿真框架，预测各种有前景的异常检测算法适配光子神经形态硬件约束后的性能。

我们将以此为基础确定基准任务，用于比较仿真得到的分类准确率、预测的能效和问题规模可扩展性，并与传统数字硬件以及其他新兴神经形态加速器上运行的现有最先进算法所报告的性能进行对比 [30]。

VII. 可靠性与安全性方面

在 NEUROPULS 中，我们将基于物理不可克隆函数，在硅级构建安全层。具体而言，我们将利用现有的光子加速器技术，实现用于构建 CMOS兼容光子物理不可克隆函数的新型架构。与基于电子技术的物理不可克隆函数相比，这类实现预计能够更好地抵御环境波动、老化、侧信道攻击和机器学习建模。这得益于光子集成电路的独特特性，例如其对温度波动或电磁干扰的依赖程度较低。其大多数组件（例如波导）在传播过程中不会出现老化问题或信号泄漏（光被限制在介电层下方的狭小区域内），而且还拥有大量可用于提升系统复杂性的自由度（相位、偏振、振幅、模式数等） [31]。

我们的研究将探讨所谓的弱物理不可克隆函数和强物理不可克隆函数 [32]：弱物理不可克隆函数方案将采用每个物理不可克隆函数仅有极少挑战的光子物理不可克隆函数设计。系统专用密钥，或系统专用的（密钥，公钥）对，将从这些弱物理不可克隆函数的（含噪）响应中导出。这里的关键方面包括前文提到的响应长期稳定性、采用最优的密钥提取和纠错技术，以及相邻光子弱物理不可克隆函数的响应在统计上的独立性。为验证这一点，将采用 NIST测试套件等统计工具 [33]。另一个重要方面是在加速器及其周边电子系统和电路中安全处理所导出的密钥。在强物理不可克隆函数方案中，必须且将采用更复杂的光子物理不可克隆函数结构。按照强物理不可克隆函数的要求，该结构应具有数量极其庞大的挑战-响应对（CRP），以及高度复杂的挑战-响应（或输入-输出）关系。在此情况下，必须利用光子物理不可克隆函数内部的非线性光学效应。

我们将系统地测试其响应的复杂性，以验证我们的光子强物理不可克隆函数设计是否具备足够的复杂性（从而具备足够的安全性）。我们将应用几种现有的强物理不可克隆函数测试，同时开发各种新测试。这些测试将评估物理不可克隆函数响应中的高阶非线性、挑战位敏感性，或通过 NIST测试套件 [33] 测量的伪随机性。评估我们的光子强物理不可克隆函数的安全性和复杂性的另一项关键策略是应用机器学习算法 [34]。给定相对较小的一组物理不可克隆函数挑战-响应对，我们将评估机器学习算法能否经过训练，预测其他尚未知的挑战-响应对。这里的关键指标包括机器学习算法训练阶段所使用的挑战-响应对数量、训练阶段的计算开销，以及经过训练的机器学习模型的预测准确率。我们将采用不同的机器学习策略，包括最新的神经网络及相关技术。我们强调，在协议和应用层面，应将弱物理不可克隆函数和强物理不可克隆函数这两种原语混合并交错使用，结合二者的优势：强物理不可克隆函数将允许系统使用长期或短期数字密钥对消息进行识别和身份验证。弱物理不可克隆函数则可在需要时用于推导秘密数字密钥，从而至少避免数字机密长期存在于硬件中 [35]。

这种硬件层面的高安全性将被用于保护软件层，即 RISC-V 处理器运行的应用代码。为此，我们将在硬件与软件的接口处设计定义明确的应用程序接口，使软件层能够向硬件层请求安全服务。这些服务包括基于秘密加密密钥执行加密、解密和数字签名任务；这些密钥绝不会泄露给软件，因此也不会泄露给潜在的恶意分析者 [36]。此外，还将开发强大的软件加固解决方案，例如程序混淆 [37]和篡改检测 [38] ，以限制针对软件组件的恶意逆向工程攻击。

VIII. 结论

NEUROPULS 项目将围绕供应链中的多个研究领域开展工作，涵盖材料科学和光子技术、计算架构、安全层以及高层次仿真。项目将开发三种不同的平台：由硅光子学驱动的芯片、基于 FPGA 并连接 RISC-V 的平台，以及用于展示神经形态加速器能力的完整仿真生态系统。这些平台的开发对于 NEUROPULS 项目至关重要，可用于展示一种基于增强型硅光子平台的低功耗安全加速器，并针对边缘计算中的三种重点用例：GNSS 抗干扰、自动驾驶和边缘设备异常检测。针对所选用例，我们的目标是将功耗降低至最先进技术水平的百分之一。我们将基于所开发的 CMOS 兼容光子平台打造新型安全层，通过紧密集成安全原语（即物理不可克隆函数）和安全软件接口来实现。此类集成将支持多种安全功能，我们会将其应用于独立运行的加速器以及特定用例。NEUROPULS 提出的模块化方法将帮助我们评估技术扩展潜力；评估时不会仅依赖硬件原型，而是通过基于 gem5 的模拟器进行精确的系统建模。项目成果将提升人们对这项技术的关注，并推动欧洲层面在光子学领域开辟新的研究方向、增加投资；光子学已被视为工业4.0和 RISC-V 处理器技术的关键赋能技术。

参考文献

[1] S. J. van Albada 等人，《数字神经形态硬件 SpiNNaker 与神经网络模拟软件 NEST 在全规模皮层微电路模型中的性能比较》，Front. Neurosci.，第 12 卷，第 291 页，2018 年 5 月。 [在线]。获取地址：https://www.frontiersin.org/article/10.3389/fnins.2018.00291/full [2] H.-T. Peng 等人，《神经形态光子集成电路》，IEEE J. Select. Topics Quantum Electron.，第 24 卷，第 6 期，第 1–15 页，2018年11月。[在线]。获取地址：https://ieeexplore.ieee.org/document/8364605/ [3] M. A. Nahmias 等人，《面向神经网络的光子乘加运算》，IEEE J. Select. Topics Quantum Electron.，第 26 卷，第 1 期，第 1–18 页，2020年1月。 [在线]。获取地址：https: // ieeexplore.ieee.org/document/8844098/ [4] Y. Shen 等人，《利用相干纳米光子电路进行深度学习》，Nature Photon，第 11 卷，第 7 期，第 441–446 页，2017年7月。 [在线]。获取地址：http://www.nature.com/articles/nphoton. 2017 93 。C. Rıos 等人，《在光子[5] ´平台上进行存内计算》，Sci. Adv.，第 5 卷，第 2 期，第 eaau5759 页，2019年2月。[在线]。获取地址：https://www.science.org/doi/ 10 1126 5759 . /sciadv.aau K. M. Ona、B. [6] Charbonnier 和 K. Hassan，《用于脉冲神经网络的硅基 III–V 族半导体激光器设计》，发表于 2021 IEEE 国际互连技术会议（IITC），2021年7月，第 1–2 页，ISSN：2380-6338。[7] R. Pappu 等人，《物理单向函数》，Science，第 297 卷，第 5589 期，第 2026–2030 页，2002年9月。 [在线]。获取地址：https://www.science.org/doi/ 10 1126 1074376 . /science. X. Xiao 等人，《在硅基 III–V 族 MOS 电容平台上实现大规模、高能效的张量化光学神经网络》，APL Photonics，第 6 卷，第 12 期，第 126107 页，2021年。[8] [在线]。获取地址：https: //doi.org/ 10 1063 5 0070913 . / . K. [9] Vandoorne 等人，《在硅光子芯片上实验演示储备池计算》，Nat Commun，第 5 卷，第 1 期，第 3541 页，2014年3月，期号：1，出版方：Nature Publishing Group。 [ ] 4541 在线。获取地址：https://www.nature.com/articles/ncomms S. Sackesyn 等人，《用于非[10] 线性光纤失真补偿的集成光子储备池计算实验实现》，Opt. Express，第 29 卷，第 20 期，第 30 991–30 997 页，2021年9月。 [在线]。获取地址：https://opg.optica.org/oe/abstract.cfm?URI = 29 20 30991 oe- - - J. [11] Feldmann 等人，《具有自学习能力的全光脉冲神经突触网络》，Nature，第 569 卷，第 7755 期，第 208–214 页，2019年5月。 [在线]。获取地址：http://www.nature.com/articles/ s41586-019-1157-8[12] M. Miscuglio 等人，《利用基于 GSST 的光子集成存储器实现具有记忆功能的人工突触》，发表于 2020 年国际应用计算电磁学会研讨会（ACES），2020年，第 1–3 页。[13] K. Mekemeza-Ona、B. Routier 和 B. Charbonnier，《基于全光调 Q 激光器的脉冲神经元》，Frontiers in Physics，第 10, 2022 [ ] 10 3389 卷。在线。获取地址：https://www.frontiersin.org/articles/ . / fphy. 2022 1017714 。G. [14] Papadimitriou 和 D. Gizopoulos，《揭开系统脆弱性栈的面纱：各层的瞬态故障效应》，发表于 2021 ACM/IEEE 第 48 届计算机体系结构年度国际研讨会（ISCA），2021年，第 902–915 页。[15] ——，《AVGI：微架构驱动的快速、精确脆弱性评估》，发表于 2023 IEEE 国际高性能计算机体系结构研讨会（HPCA），2023年，第 935–948 页。[16] P. R. Bodmann 等人，《ARM 微处理器的软错误效应：早期估算与芯片测量结果比较》，IEEE Transactions on Computers，第 71 卷，第 10 期，第 2358–2369 页，2022年。[17] Y. J. Morton 等人，《21 世纪的定位、导航与授时技术：集成卫星导航、传感器系统与民用应用》，John Wiley & Sons，2021年。[18] M. G. Amin 等人，《基于卫星的导航系统中的漏洞、威胁与身份验证 [本期导读],》，Proceedings of the IEEE，第 104 卷，第 6 期，第 1169–1173 页，2016年。[19] R. Morales-Ferre 等人，《有人与无人驾驶航空器卫星导航中应对蓄意干扰的综述》，IEEE Communications Surveys Tutorials，第 22 卷，第 1 期，第 249–291 页，2020年。[20] R. M. Ferre、A. D. L. Fuente 和 E. S. Lohan，《利用机器学习算法对 GNSS 频段中的干扰器进行分类》，Sensors (Switzerland)，第 19 卷，第 22 期，第 5–7 页，2019 年。

[21]G.-H. Lee、J. Jo 和 C. H. Park，《使用机器学习方法预测雷达信号中的干扰》，《安全与通信网络》，第2020卷，页1–9，2020年1月。 [在线]。网址：https://www.hindawi.com/journals/scn/2020/2151570/ [22] P. Wu 等，《基于联邦学习的干扰器分类》，发表于 IEEE/ION PLANS 会议论文集，加利福尼亚州蒙特雷，2023年4月。[23] ApolloAuto。（2018）Apollo 3.0软件架构。 [在线]。网址：https://github.com/ApolloAuto/apollo/blob/master/docs/ specs/Apollo [24] T. A. Foundation，《Autoware：一个开放的自动驾驶平台》。https://github.com/CPFL/Autoware/，2016年。[25] M. Cajamarca，《用于目标轨迹预测的基于 Keras 的多输入多输出 LSTM 循环神经网络》，https://github.com/MarlonCajamarca/ Keras-LSTM-Trajectory-Prediction，2022年。[26] Y. Meidan 等，《N-BaIoT：基于网络的检测方法，利用深度自编码器检测物联网僵尸网络攻击》，《IEEE普适计算》，第17卷，第3期，页12–22，2018年。[27] R. Doriguzzi-Corin 等，《Lucid：一种实用、轻量级的深度学习解决方案，用于DDoS攻击检测》，《IEEE网络与服务管理汇刊》，第17卷，第2期，页14，2020年。[28] Y. Jaoudi、C. Yakopcic 和 T. Taha，《将无监督异常检测系统转换为脉冲神经网络以识别汽车黑客攻击》，发表于2020年第11届国际绿色与可持续计算研讨会（IGSC），2020年，页1–4。[29] Q. Chen 等，《AnRAD：面向海量并发数据流的神经形态异常检测框架》，《IEEE神经网络与学习系统汇刊》，第29卷，第5期，页1622–1636，2018年。[30] Y. Yan 等，《在低延迟关键词检测和自适应机器人控制方面比较 Loihi 与 SpiNNaker 2 原型》，《神经形态计算与工程》，第1卷，第1期，页014002，2021年7月。 [ ] 10 1088 2634 4386 150 在线。网[31] 址：https://dx.doi.org/ . / - /abf F. Pavanello 等，《光子物理不可克隆函数的最新进展》，发表于2021年IEEE欧洲测试研讨会（ETS）。比利时布鲁日：IEEE，2021年5月，页1–10。 [在线]。网址：https: // ieeexplore.ieee.org/document/9465434/ [32] U. R¨uhrmair 和 D. E. Holcomb，《物理不可克隆函数概览》，发表于2014年欧洲设计、自动化与测试会议暨展览（DATE）。IEEE，2014年，页1–6。[33] A. Rukhin 等，《用于密码学应用的随机数和伪随机数生成器统计测试套件》，Booz Allen Hamilton公司（弗吉尼亚州麦克莱恩），技术报告，2001年。[34] U. R¨uhrmair 等，《针对仿真数据与硅芯片数据的物理不可克隆函数建模攻击》，《IEEE信息取证与安全汇刊》，第8卷，第11期，页1876–1891，2013年。[35] U. R¨uhrmair，《无秘密安全：综述与教程》，《密码工程期刊》，第12卷，第4期，页387–412，2022年。[36] M. Ceccato 等，《了解黑客在专业环境和公开挑战中执行攻击任务时的行为》，《实证软件工程》，第24卷，第1期，页240–286，2019年2月。 [在线]。网址：https://doi.org/10.1007/ s10664-018-9625-6[37] ——，《代码混淆对 Java 代码质量影响的大规模研究》，《实证软件工程》，第20卷，第6期，页1486–1524，2015年。 [在线]。网址：http://dx.doi.org/10.1007/ s10664-014-9321-0[38]A. Viticchi´e 等，《反应式认证：自动检测并应对软件篡改攻击》，发表于2016年ACM软件保护研讨会论文集，系列SPRO ’16。美国纽约州纽约市：ACM，2016年，页73–84。 [在线]。网址：http://doi.acm.org/10.1145/2995306.2995315