预印本——已被第21届IEEE Interregional NEWCAS Conference接收。

arXiv:2304.05682v1 [cs.CR] 12 Apr 2023

集成式存内计算模块的自动化信息流分析

Lennart M. Reimann、Felix Staudigl 和 Rainer Leupers 亚琛工业大学{lennart.reimann、staudigl、leupers}@ice.rwth-aachen.de

摘要——新型非易失性存储器（NVM）技术可实现高速、高密度的数据存储。此外，它们通过实现存内计算（CIM）克服了冯·诺依曼瓶颈。人们提出了多种计算机架构，将存内计算模块集成到设计中，形成混合信号系统，从而结合存内计算的计算优势与传统 CMOS 的稳健性。设计和制造这类神经形态系统，需要新型电子设计自动化工具（EDA tools）。此外，鉴于近年来硬件安全攻击日益增多，电子设计自动化工具还必须考虑安全漏洞的影响。现有的信息流分析框架可提供自动化工具套件，在硬件设计过程中维护敏感数据的机密性属性。然而，目前可用的混合信号电子设计自动化工具无法分析神经形态系统的信息流。为展示其不足，我们为非易失性存储器制定了信息流协议，这些协议可轻松集成到现有工具套件中。我们通过分析敏感信号经过多个忆阻交叉阵列结构流向潜在不可信组件和输出的过程，展示了当前最先进技术的局限性。最后，我们全面讨论了混合信号信息流分析框架在神经形态系统中的优缺点。

索引词——信息流分析、神经形态计算、机密性

I. 引言

非易失性存储器（NVM）技术，例如自旋转移力矩存储器（STT-RAM/MRAM）、相变随机存取存储器（PCRAM）或氧化还原型随机存取存储器（ReRAM），是取代传统 RAM 的有前景候选方案。非易失性存储器具有高密度存储和低漏电功耗的优势，并支持存内计算。

将传统CMOS 与非易失性存储器相结合，会产生称为神经形态系统的复杂高性能设计。在现代设计流程中，电子设计自动化工具用于协助设计人员完成复杂的实现工作。然而，电子设计自动化工具需要配备相应功能，以便支持集成基于非易失性存储器的加速器的混合信号设计。此外，新型技术引入了新的安全漏洞（见图 1） [1]–[3]。这些新漏洞尤其令人担忧，因为神经形态系统是未来应用的有前景候选方案，例如自动驾驶。因此，需要对电子设计自动化工具进行调整，以便为混合信号设计强制实施安全属性，从而在数字域和模拟域中实现安全感知的设计流程。可用性、机密性和完整性是硬件安全的三大基石，必须在设计过程中加以考虑。尽管大多数研究聚焦于完整性属性 [4], [5],

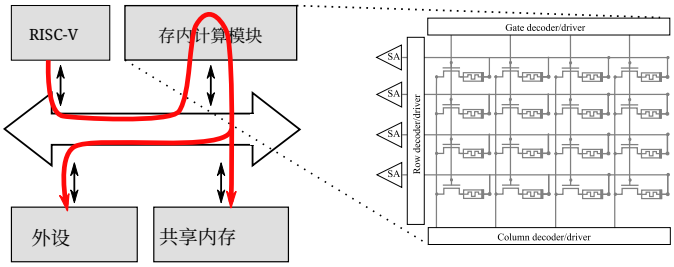


图 1：使用存内计算模块（1T1R交叉开关阵列）的 SoC 中典型的数据泄漏路径。敏感数据从可信源（RISC-V）流向不可信的外设或共享存储器。

我们的工作重点关注机密性属性。信息流分析（信息流分析）是设计中强制实施机密性属性和完整性属性的最先进技术。信息流分析可以跟踪信息从敏感源（例如加密密钥）流向不受信任组件（例如输出或第三方知识产权（IP））的过程。该分析可以静态执行，以确保对于每种可能的输入组合，信号的机密性。尽管已有一些支持混合信号设计的研究发表，但据我们所知，尚无研究讨论非易失性存储器的信息流。因此，我们的工作扩展了当前可用的、面向神经形态混合信号系统的信息流分析工具，并讨论了其优点和缺点。

本文的主要贡献如下：（1）为 NVM 组件制定信息流策略。（2）介绍一种交叉开关阵列驱动器屏蔽方案，以禁止硬件中的潜行路径。（3）展示当前面向神经形态系统的混合信号信息流分析工具的局限性。

II. 背景

A. 信息流分析

信息流分析是硬件设计中确保完整性和机密性属性的最先进技术。安全分析要求将硬件划分为不同的安全类别并进行标记。例如，第三方 IP、共享资源或设计的输出端口会被标记为不可信。信息流分析用于确定来自高安全级别部分的信息是否会影响低安全级别区域。该分析基于非干扰属性，旨在证明敏感值的变化不会导致不可信组件出现可观察到的变化。敏感信号不会干扰不安全组件。在设计的每个阶段强制执行这些属性。

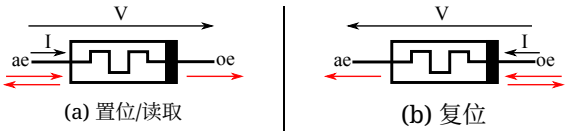


图 2：不同工作模式下忆阻器中的信息流（红色箭头）。

流程，避免可能威胁敏感数据（如加密密钥或用户数据）的安全漏洞。

B. VeriCoq-IFT

大多数信息流分析框架都用于处理数字硬件。相比之下，VeriCoq-IFT 框架 [6]引入了在分析信息流 [7]时处理混合信号设计的能力。分析会判定敏感信息是否泄漏到设计的输出信号中。首先，必须将设计的所有输出端口标记为不可信。其次，用户在设计描述中标记敏感信号，并为其分配敏感度分数。VeriCoq-IFT 采用保守的方法，在 Verilog 中每次进行信号赋值时，都会传播该信号的敏感度分数。变量会获取其所有输入中最高的敏感度分数。此外，操作可以标记为敏感度降低器，因此每当敏感信号经过指定操作时，其敏感度分数都会降低。如果信号在敏感度分数降至零之前到达输出端口，就会检测到数据泄漏。该分数系统可用于确保明文在作为密文到达设计输出端口之前，至少经过 12 轮 AES 运算。然而，针对忆阻器的信息流规则尚未提出。

C. 非易失性存储器（NVMs）

非易失性存储器是一种新型存储技术，利用了忆阻器。忆阻器与电容器、电阻器和电感器并列，是第四种基本电气元件，并以电阻的形式存储信息。电阻可通过电压脉冲进行置位或复位，不同的电阻值代表不同状态，分别称为低阻态（LRS）和高阻态（HRS）。为了实现高密度存储，忆阻器被组织成由水平字线和垂直位线构成的交叉阵列结构，每个交叉点上都设有一个忆阻单元。这类所谓的无源交叉开关阵列会受到忆阻单元之间寄生效应所导致的潜行路径电流影响，从而限制其可靠性和保持特性。因此，人们提出了更先进的单元结构，其中集成了有源元件（即晶体管），用于将忆阻器与交叉阵列的其余部分连接或隔离。然而，由于这些新型器件尚未在 VeriCoq-IFT 框架中讨论过， [7], 因此需要制定并实现信息流策略，以便分析神经形态系统中的信息流。

III. 威胁模型

所开发的框架旨在识别神经形态混合信号设计中的不必要信息泄漏。该

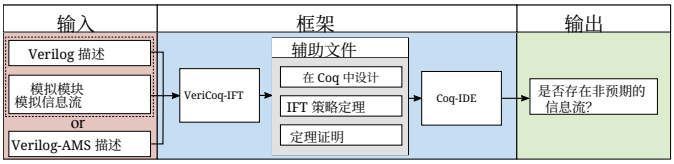


图 3：本文中 VeriCoq-IFT [6] 和 CoqIDE [10]的功能。

对数字组件在寄存器传输级进行静态分析，对模拟部分在晶体管级进行分析。我们假设攻击者可以访问完整的硬件描述，并试图通过主输出处的信息直接流出泄露信息，无论这些输出位于模拟域还是数字域。侧信道不在考虑范围内。我们假设硬件漏洞在设计阶段就已存在。不考虑主输出的观测是通过远程访问还是物理访问获得的。

IV. 相关工作

Khan 等人详细阐述了针对新兴非易失性存储器的信息泄漏所可能发起的攻击：在读写敏感数据时，利用电源噪声引发的侧信道进行攻击 [8]。此外，当前研究表明，依赖于数据内容的写入延迟可被用作侧信道，泄漏敏感信息。通过观察访问忆阻器所需的时间，可以推断出当前存储内容的相关信息。针对这一安全漏洞的分析也曾通过人工方式进行 [2]。除了利用电源噪声和写入延迟进行侧信道攻击外，还可以通过监测电源电流来获取有关敏感信号的信息 [1]。

尽管非易失性存储器中已发现多种安全漏洞，但目前尚无工作提出自动识别此类漏洞的方法。我们需要具备安全感知能力的自动化电子设计自动化工具，以协助缺乏硬件安全经验的硬件设计人员识别安全漏洞，同时保持有竞争力的设计流程。

V. 框架

因此，我们为非易失性存储器制定了信息流规则，并将其集成到已有的信息流分析框架中。图 2 展示了忆阻器在三种工作模式——置位、读取和复位——下电压与电流的方向。置位和读取时，从端子 ae 对忆阻器进行访问，因此电流和电压的方向均指向另一端子，在本文中称为 oe 。从根本上说，忆阻器还需要第四种模式，以便在制造后初始化器件。然而，由于与其余工作模式相比，该模式的攻击面有限，因此本文不予考虑。

如[7], 所述，对于模拟组件，信息通过电压和电流传递。因此，在 ae处设置电压时，可以通过电流从忆阻器的两个端子读取信息。由于忆阻器的双向行为， [9], 信息流呈现双向特性，如图 2 中三个访问模式的红色箭头所示。

```
1 // 模拟信息流2 // 在忆阻器中3 module memri
stor(ae,oe);4 inout ae,oe;56 assign ae =
ae |oe;7 assign oe =ae |oe;8
endmodule
```

图 4：对信息流进行建模的 Verilog 忆阻器模块的高级定义。

我们将推导出的策略集成到 VeriCoq-IFT 中，并将该框架直接与 CoqIDE [10] 结合，以提供自动化信息流分析框架。本工作用于评估的 VeriCoq-IFT 与 CoqIDE 组合框架的工具流程如图 3 所示。尽管 VeriCoq-IFT 最初面向第三方知识产权，被设计为证明携带型硬件知识产权，但在本工作中，它仅用于信息流分析。VeriCoq-IFT 有两种工作模式：1）处理完整设计的 Verilog-A/MS 描述；或 2）由设计者提供数字域的 Verilog 描述，以及模拟模块的 Verilog 模块，以模拟器件的信息流。后一种模式适用于设计早期阶段，此时尚无忆阻器的 Verilog-A/MS 描述。因此，需要引入用于模拟忆阻器信息流的 Verilog 模块。该模型并不描述非易失性存储器件的实际行为，而是对信息流进行建模。图 4 展示了用于模拟忆阻器信息流的 Verilog 模块。两个端子 ae 和 oe 均标记为 “inout” 端口。此外，两个端口分别都依赖于两个端子（第 6 行和第 7 行）。Verilog赋值语句右侧所执行的操作类型并不重要，因为只需对信息流进行建模，而非对功能进行建模。这使该框架能够在数字域中处理模拟忆阻器。

其次，现代电子设计自动化工具支持将混合信号设计导出为 Verilog-A/MS 语言。元件的模拟和数字行为被嵌入到同一份描述中。网上提供少量 Verilog-A/MS 器件 [11]。VeriCoq-IFT 会处理该设计，生成 Coq 语言的设计描述，以及信息流规则的定理和证明。这些规则针对设计描述中所有标记为敏感的信号生成。在本研究中，所有敏感度标签均设为 1，且未实例化任何敏感度降低器，从而保证非干扰属性 [12]。因此，任何可能受敏感信号影响的输出端口都会被标记为泄漏点。随后，将这三个辅助文件提交给 CoqIDE 中的定理证明器。如果硬件描述在 Coq 中的定理和证明均通过，则未检测到泄漏；否则，VeriCoq-IFT 会识别出非预期的信息流。

VI. 演示

在这项工作中，我们通过三个独立的、基于集成式 NVM 的混合信号设计，展示了所提出框架的功能与局限性。我们假设 NVM 模块集成在片上系统（SoC）加速器中。我们着重评估模拟域，以展示所实现框架的能力与不足。图 5 展示了 SoC 的模拟域，并用红色标示出一条已识别的泄漏路径。在这个示例设计中，周边电路支持对无源和有源交叉开关阵列的编排。接下来，我们进行三项实验，以突出信息流分析（IFA）应用于神经形态系统时面临的障碍，以及 IFA 框架的不足。图 5(b) 和 (d) 展示了两种交叉阵列结构的内部细节。通过替换蓝色的抽象交叉开关阵列，这两种交叉阵列结构均可集成到电路中（图 5(a)）。此外，我们提出一种掩码机制，以强制按预期方式使用 NVM 模块（见图 5(c)）；该机制将取代图 5(a) 中所示的驱动器。

A. 1R交叉开关阵列加速器

无源交叉开关阵列的存储单元由单个忆阻器构成。因此，交叉开关阵列本身就像一个电阻网络，允许双向信息流。数字域根据已实现的输出信号限制信息流，即执行向量矩阵乘法，或通过输入信号传递结果。图 5 (b) 用红色示例展示了一条除预期信息流之外可能存在的信息泄漏路径。除了从 到 的预期信息流外，也识别出了非预期的潜行路径（参见 到 ）[13]。总的来说，无源交叉开关阵列中的信息流被认为十分复杂，因为其方向并不明确，而且信息可以在模拟域和数字域之间交替传输。

B. 1T1R交叉开关阵列加速器

虽然无源交叉开关阵列会产生潜行路径电流，限制其可用性，但有源交叉开关阵列旨在通过为 NVM 单元添加有源元件 [13]来解决这一问题。图 5 (d) 展示了一个有源交叉开关阵列，其中使用晶体管作为选择器元件，将未选中的单元与交叉开关阵列隔离开来。然而，我们的实验表明，由 VeriCoq-IFT 确定的有源交叉开关阵列的信息流与无源交叉开关阵列的信息流相同。VeriCoq-IFT 对设计进行静态分析，但不会考虑选择器晶体管的“预期”用途。因此，该框架将 NVM 模块判定为存在泄漏。

C. Active Crossbar Accelerator with Access Mask

为确保通过交叉开关阵列的信息流，我们提出了一种硬连线访问掩码，用于强制选择器晶体管按照预期方式使用。我们在 NVM 模块的驱动电路中实现了该访问掩码。该掩码仅允许将一组固定的驱动电压施加到交叉开关阵列，如表 I 所示，并通过查找表实现（见图 5(c)）。该查找表禁止能够同时写入多行的工作模式，从而消除潜行路径。例如，当访问第 m 行和第 n 列（绿色）中的忆阻器时，所有其他字线和位线均设置为 GND（橙色），从而阻断潜在的潜行路径。

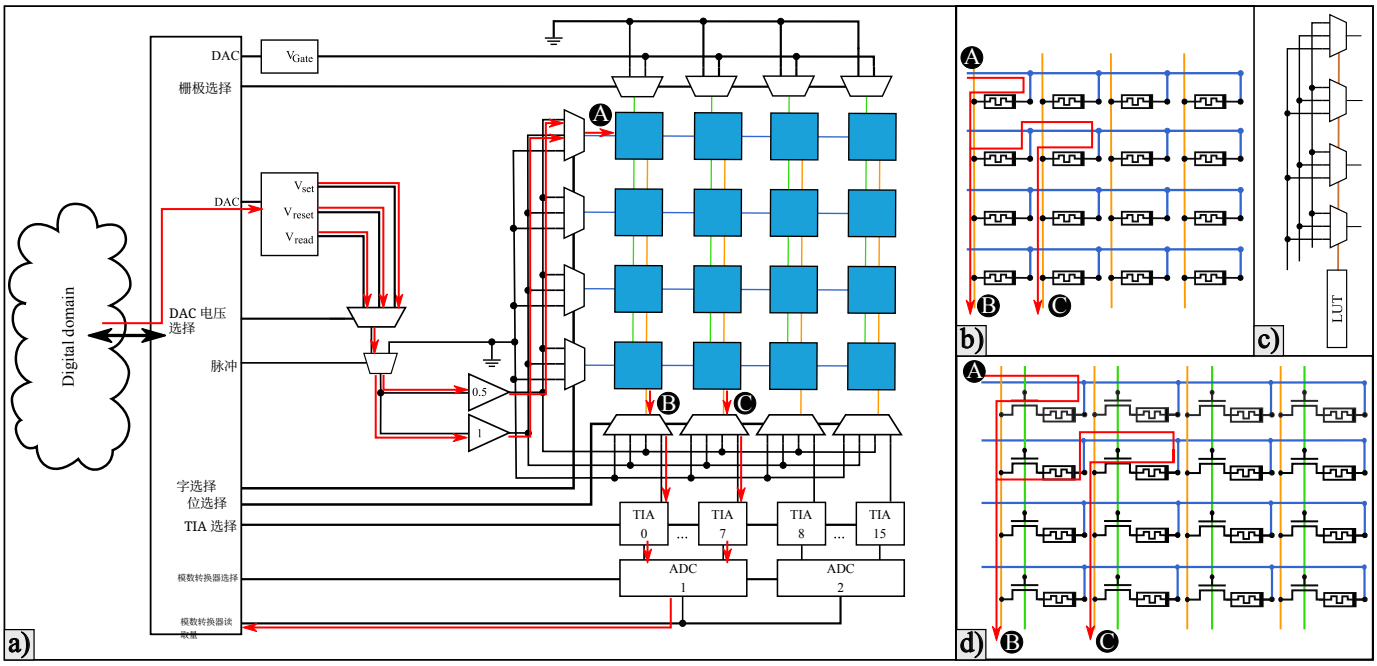


图 5：演示设置：(a) 存内计算模块及其与数字域的接口，其中包含通用交叉开关阵列（蓝色）；(b) 可集成到左侧存内计算模块中、用于通用交叉开关阵列的 1R交叉开关阵列；(c) 用于驱动器、禁止某些电压组合的查找表；以及 (d) 可集成到左侧存内计算模块中的 1T1R交叉开关阵列。红线表示数字域中敏感信号的示例性泄漏，这些泄漏由我们的 VeriCoq-IFT 设置识别。

VeriCoq-IFT 分析的结果通过红色泄漏路径展示（图 5(d)），这些路径与前两种硬件设计中的相同。

VII. 讨论

对 1R交叉开关阵列进行 VeriCoq-IFT分析能够准确描述潜行路径的行为，因此该框架可以识别潜在的数据泄漏。相反，有源交叉开关阵列通过引入晶体管等有源元件，解决了潜行路径电流的影响。由于静态分析无法描述有源与无源交叉开关阵列之间的差异，信息流并未改变。尽管控制电路中的访问掩码必然会导致识别出的信息流发生变化，但 VeriCoq-IFT 的保守分析无法区分这三种设计的信息流，因而产生误报识别。具体而言，包含存内计算模块的片上系统设计允许信息流在模拟域和数字域之间连续流动，因此需要采用更宽松的方法，以减少大量

表 I：使用 (m,n)-交叉开关阵列时，在(k,l) 处设置或复位交叉开关阵列所允许的访问掩码规则。

SET	复位
$V_{WL,k} = V_{SET}$	$V_{WL,k} = V_{RES}$
$V_{SL,l} = V_{GAT}$	$V_{SL,l} = V_{GAT}$
$V_{BL,l} = GND$	$V_{BL,l} = GND$
$V_{WL,1:k-1} = GND$	$V_{WL,1:k-1} = GND$
$V_{SL,1:l-1} = GND$	$V_{SL,1:l-1} = GND$
$V_{BL,1:l-1} = GND$	$V_{BL,1:l-1} = GND$
$V_{WL,k+1:m} = GND$	$V_{WL,k+1:m} = GND$
$V_{SL,l+1:n} = GND$	$V_{SL,l+1:n} = GND$
$V_{BL,l+1:n} = GND$	$V_{BL,l+1:n} = GND$

误报。数字域已有更宽松的方法 [14],，但模拟域仍缺少此类方法。精确的框架会考虑信号间的依赖关系、操作的实际功能以及信号的精确值，而 VeriCoq-IFT 并未做到这一点。因此，需要开发一种框架，通过处理 Verilog-A/MS 描述中的信息，考虑模拟域中的上述特征。

VIII. 结论

本文评估了面向集成计算存内模块的先进信息流分析框架 VeriCoq-IFT。如文中所示，可以实现派生的 Verilog 模型，从而对新兴的忆阻器交叉阵列进行早期阶段的信息流分析；这类阵列是神经形态系统的重要构建模块。本文通过三个系统设计展示了混合信号信息流分析的功能。然而，当前模拟信息流定理具有保守性，因此会产生大量误报，使得对存内计算模块中机密性属性进行实用静态分析变得不可行。未来工作可以扩展该框架，以支持对信息流进行不那么保守的分析 [14]，甚至量化信息流，从而忽略可忽略不计的信息流 [15], [16]。

致谢

该工作由德国联邦教育与研究部（BMBF）在 NEU-ROTEC II 项目框架内资助，合同编号为 16ME0399。VeriCoq 框架由达拉斯德克萨斯大学的 TRELA 实验室提供。

参考文献

[1] M. N. I. Khan 等人，“面向密码学应用的基于 STTRAM 的缓存侧信道攻击”，载于《2017 年 IEEE 国际计算机设计会议（ICCD）》，2017 年，第 33–40 页。[2] J. Krautter 等人，“忆阻器缓存中通过自终止写入方案导致的数据泄漏”，载于《2022 年第 27 届亚洲及南太平洋设计自动化会议（ASP-DAC）》，2022 年，第 666–671 页。[3] C. Yang 等人，“挫败针对基于忆阻器的神经形态计算系统的复制攻击”，《IEEE 集成电路与系统计算机辅助设计汇刊》，第 39 卷，第 10 期，第 2192–2205 页，2020 年。[4] F. Staudigl 等人，“NeuroHammer：在忆阻器交叉开关阵列存储器中诱发位翻转”，载于《2022 年欧洲设计、自动化与测试会议暨展览会（DATE）》，2022 年，第 1181–1184 页。[5] F. Staudigl 等人，“X-Fault：故障对采用存内逻辑计算的忆阻器交叉开关阵列中二值神经网络的影响”，2022 [ ] 2204 01501 。在线。可访问：[6] https://arxiv.org/abs/。M. Bidmeshki 等人，“面向第三方硬件 IP 信息流策略的自动化证明生成”，载于《2015 年 IEEE 硬件导向安全与信任国际研讨会（HOST）》，2015 年。[7] M. M. Bidmeshki 等人，“基于证明携带硬件的模拟/混合信号设计信息流跟踪”，《IEEE 新兴与精选电路和系统期刊》，第 11 卷，第 2 期，2021 年。[8] M. N. I. Khan 等人，“新兴非易失性存储器的信息泄漏攻击及对策”，载于《论文集》国际低功耗电子与设计研讨会论文集，系列 ISLPED ’18。美国纽约州纽约市：计算机协会，2018年。 [在线]。可访问：https://doi.org/ 10 1145 3218603 3218649 。/。F. Cuppers 等人，“利用 HfO 2 [9] .. 基 ReRAM 器件的开关动态实现可靠的模拟忆阻器行为”，《APL Materials》，第7卷，第091105页，2019年9月。[10] Inria、CNRS 及贡献者，“CoqIDE”，2021年。 [在线]。可访问：https://coq.inria.fr/refman/practical-tools/coqide.html [11] Electronic Materials Research Laboratory，“JART”，2021年。 [在线]。可访问：https://www.emrl.de/JART.html [12] P. Ryan 等人，“非干扰性，谁需要它？”，载于《第14届 IEEE 计算机安全基础研讨会论文集》，2001年。[13] M. A. Zidan 等人，“基于忆阻器的存储器：潜行路径问题及其解决方案”，《Microelectronics Journal》，第44卷，第2期，第176–183页，2013年。[在线]。可访问：https://www.sciencedirect.com/science/article/pii/S 0026269212002108 [14] D. Zhang 等人，“面向时序敏感信息流安全的硬件设计语言”，《SIGARCH Comput. Archit. News》，第43卷，第1期，第503–516页，2015年3月。 [在线]。可访问：https://doi.org/ 10 1145 2786763 2694372 。/。[15] L. M. Reimann 等人，“QFlow：Verilog 中面向安全感知硬件设计的定量信息流”，载于《2021 IEEE 第39届国际计算机设计会议（ICCD）》，2021年，第603–607页。[16] L. M. Reimann 等人，“面向硬件的定量信息流：推进攻击版图”，2022年。 [在线]。可访问：https://arxiv.org/abs/2211.16891