

EEPROM 的扫描电镜探测和探针攻击

程 鹏, 白国强

(清华大学微电子与纳电子学系, 北京 100084)

摘 要: 阐述两种针对芯片的侵入式攻击方法, 即扫描电镜(SEM)探测和探针攻击. 攻击的目标都是从 EEPROM 中提取数据内容, EEPROM 因为通常会存储认证信息和个人密钥等敏感信息. 描述两个实验过程, 第一个实验利用非易失性存储器的存储特点, 对一个通用存储器芯片进行预处理后直接使用 SEM 进行观测, 试图从图像上辨别不同存储状态的单元并且定位单个存储器单元; 第二个实验对某款芯片预处理后, 针对单个 EEPROM 存储器单元晶体管各端口进行电学连接, 制作焊盘(PAD), 之后使用探针探测存储器单元工作电信号, 从而区分不同状态的单元.

关键词: 侵入式攻击; EEPROM; SEM; 内容提取; 探针探测

中图分类号: TN307

文献标识码: A

文章编号: 1000-7180(2016)03-0037-04

EEPROM Memory SEM Search and Probing Attack

CHENG Peng, BAI Guo-qiang

(Institute of Microelectronics, Tsinghua University, Beijing 100084, China)

Abstract: This paper proposed two invasive attack methods against semiconductor chips, and these two methods are SEM search and probing attack, respectively. Their goals are both extracting contents from EEPROM which usually keeps sensitive information such as authentication information and personal keys. Two experiments process were shown in this paper. By making use of features of nonvolatile memories, the first one used SEM to observe target EEPROM cells to distinguish cells which store different contents and to locate EEPROM cells with certain memory chip pre-processed. The second one used needles to test working signals of memory cells by contacting PADs which connect electrodes of memory cell transistors to distinguish different cells.

Key words: invasive attack; EEPROM; SEM; content extracting; probing attack

1 引言

半导体芯片是信息安全保护的关键, 半导体芯片使用非易失性存储器, 通常是 EEPROM 或者 Flash 来长时间存储敏感数据, 例如验证信息, 加密密钥及其他重要数据^[1], 所以 EEPROM 或者 Flash 存储安全是芯片安全的中中之重. 为了提高芯片的存储安全, 首先掌握攻击可以更有效地设计防御策略. 攻击方法通常分三类, 其中侵入式攻击公开发表研究成果基本没有, 但是此类攻击手段直接, 效果明显. 因此, 本文从侵入式攻击手段的角度出发, 提出了针对 EEPROM 的扫描电镜探测和探针攻击方法

并且进行了实验验证.

2 背景

高安全性芯片 EEPROM 中存储的敏感信息无法输出片外, 针对这类芯片的攻击手段可以分为三类: 非侵入式攻击、半侵入式攻击与侵入式攻击^[2]. 其中, 非侵入式攻击的攻防研究丰富, 后两种攻击特别是侵入式攻击对设备要求较高, 而且工程难度大, 研究成果少. 然而, 后两种攻击却有着无可替代的优势^[3].

2.1 非易失性存储器

非易失性存储器基本单元有两种类型, 分别是电荷陷阱设备和浮栅设备, 后文以浮栅结构为例进

行说明.

目前最主流两种非易失性存储器是 EEPROM 和 Flash. EEPROM 以字节为单位进行内容读取以及所有的编程操作,存储器单元由一个浮栅晶体管以及一个选择晶体管组成,也被称为两晶体管存储器单元,单元结构如图 1 所示^[4]. 通过给各个端口加适当电压可以实现编程,擦除该操作.

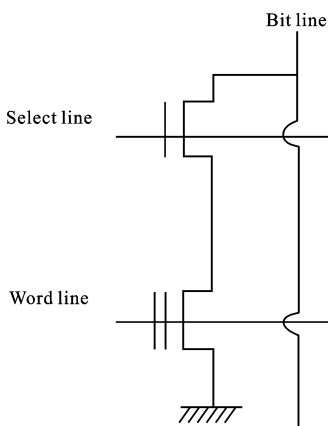


图 1 EEPROM 的结构示意图

2.2 侵入式攻击

侵入式攻击需要对芯片进行“开盖”,去封装,甚至去金属层等操作,通常对芯片造成不可逆破坏.这类攻击主要分为逆向工程和探针探测攻击.前者用于分析电路功能和组成结构等,后者是主要的侵入式攻击方法.探针探测原理简单,即使用探针来接触芯片内部信号线或者探测芯片内部感兴趣部分的电信号,必要时需要用聚焦离子束(FIB)设备制作焊盘(PAD),将信号线从下层金属层引到芯片表面方便探测.

3 攻击原理

本文针对 EEPROM 设计了两种侵入式的探测和攻击方法.

第一部分工作将失效分析通常使用的扫描电镜(SEM)与芯片安全结合,尝试使用 SEM 直接提取 EEPROM 存储信息以及探索 SEM 对存储器晶体管进行探测与定位的作用.

SEM 的工作原理是:SEM 发出电子束,轰击在样品表面后,产生二次电子,背散射电子和俄歇电子等粒子在内的信号.在 SEM 加装探头选择性接收信号成像,就能根据接收的是何种粒子得到着重反映样品表面信息的图像.由于成像的分辨率高,通常收集二次电子信息.

本文提出的 SEM 探测的原理是:对于非易失性存储器,以浮栅型器件为例,由于不同存储状态的存

储器单元浮栅上的电子数目不同,使用 SEM 观察存储器单元时,如果不同数目的浮栅电子对产生二次电子影响不同,那么这些二次电子形成的图像也会有区别.于是就可以直接从图像上区别浮栅上的不同电子数目,从而区别不同存储状态的存储器单元.探测过程如图 2 所示.

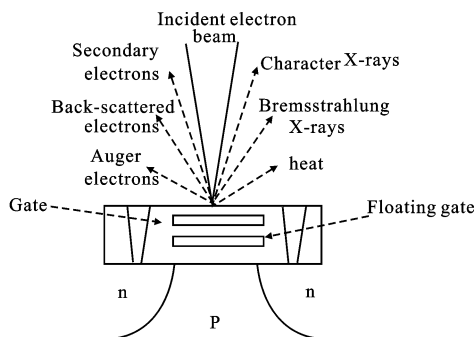


图 2 SEM 探测原理图

这种方法的限制:电子束轰击样品表面只能够直接作用到顶层控制栅,因此需要寻找方法使得电子束能够作用到浮栅的位置,才能获得收到浮栅上电子影响的二次电子的信息.

第二部分工作的工作原理是:把目标直接定位为 EEPROM 中单独的单元.给每个存储器单元各端口加电信号激励,提供读存储器单元时的条件,从而根据测试得到的 I-V 曲线来判断存储单元存储的内容.探针攻击示意图如图 3 所示.实际攻击时,往往无法做到将探针连接到各端口上,需要使用 FIB 设备从目标区域引线到可探测区域并制作 PAD.探针直接从 PAD 探测信号.由于存储不同内容的存储器阈值电压不同,因此会出现图 4 所示的结果.

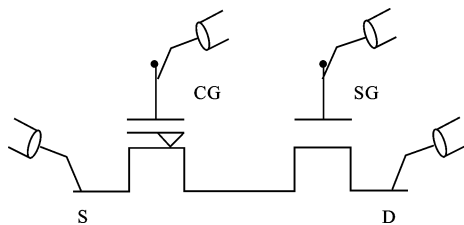


图 3 探针攻击示意图

4 实验准备

实验一选择 Atmel 公司生产的 AT24C128,一款通用纯存储器芯片.攻击前,需要给存储器存储便于攻击的数据内容.

根据 AT24C128 的用户手册,通过微控制器给芯片存入特殊形式数据,特殊形式为相邻数据页

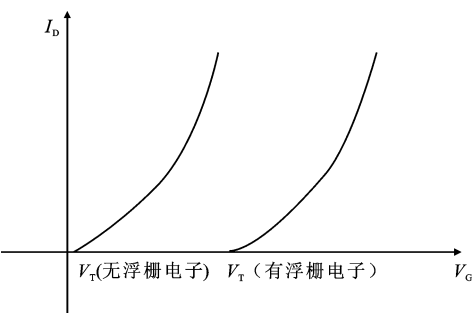


图 4 不同内容存储器 I-V 曲线差别

存储不同内容,这样存的目的是为了后续观测方便.

首先需要对芯片进行预处理:由于需要尽可能使 SEM 电子束轰击到接近浮栅的区域,因此需要将芯片 Die 取出,并且去封装去金属层. 由于 EEPROM 是非易失性存储器,所以这些操作并不会影响数据完整性,取出 Die 之后使用光学显微镜拍摄到芯片表面如图 5 所示,图中标示出了 EEPROM 区域. 该芯片共有三层金属层,去除金属层后显露出的多晶硅层如图 6 所示.

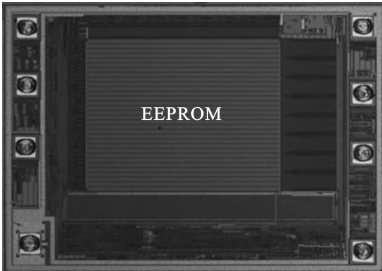


图 5 AT24C128 芯片表面

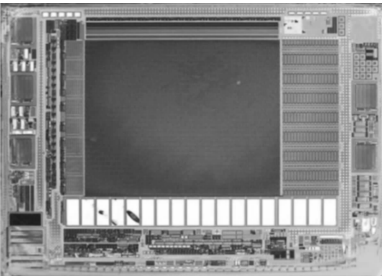


图 6 AT24C128 多晶硅层

使用 SEM 观察之前,先使用光学显微镜进行存储器最小区域定位,通常光学显微镜最大放大倍数为 1 000 倍,使用最大倍数尽力找到最小存储区域,之后再使用 SEM 做进一步观察. 需要注意,由于机理问题,SEM 对物体表面穿透性不强,需要调节电压进行一定程度的调节.

实验二使用某款射频用芯片,实际探针探测之

前需要做一系列预处理. 首先对芯片表面进行开盖. 因为需要使用探针给 EEPROM 的存储单元各个电极人为施加激励,所以需要现在芯片表面合适位置制作焊盘并且和目标晶体管各端进行电学连接,制作 PAD.

为了制作 PAD,需要了解实际芯片各个区域电路结构. 由于没有关于芯片的资料,所以先对芯片进行了一定程度的逆向分析,从而分析出 EEPROM 阵列的形式结构和制作 PAD 的位置. 图 7 所示为攻击的 EEPROM 阵列结构,图 8 中白色方框为经过分析后确定的 PAD 区域的示意图.

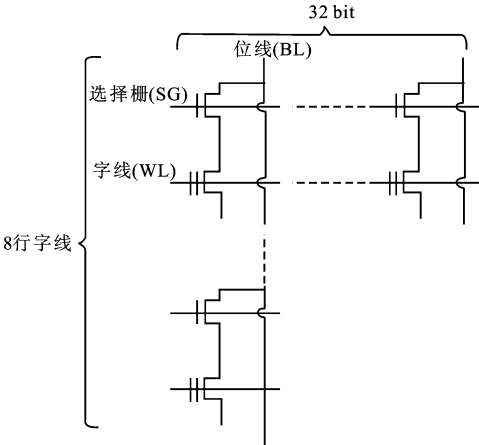


图 7 EEPROM 阵列结构

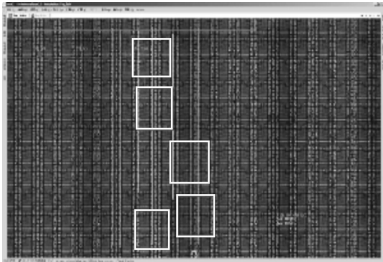


图 8 制作 PAD

PAD 制作完毕之后,芯片预处理结束,开展实际探针探测. 探针探测需要使用探针台,本实验使用 Cascade 公司的 Summit11000 探针台,并且配备 Agilent B1500 半导体分析仪进行攻击.

由于缺乏芯片 EEPROM 区域资料,因此需要估计给晶体管各端施加的激励大小,具体数值如表 1 所示,其中 Hiz 表示高阻状态.

表 1 探针探测激励具体参数				V
Operation	V_{SG}	V_{CG}	V_D	V_S
Program	16	0	15.5	Hiz
Read	3.3	1.8	BL	0

5 实验过程与结果

实验一准备工作完毕后,首先使用光学显微镜观察最小存储器区域,结果如图 9 所示.结合用户手册分析,图中方框区域中共存在 8 个浮栅晶体管单元.

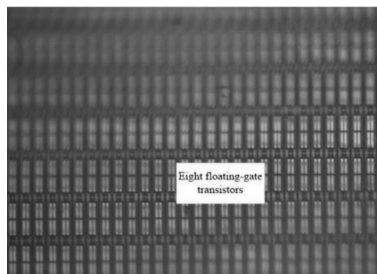


图 9 光学显微镜定位结果

使用 SEM 在放大 12 000 倍时进行观测,结果如图 10.图 10 中白色方框包围区域和图 9 中白框区域是同一个位置.在图中只能看到黑色不透明区域以及白色的点,白色的点是连接被离的上层金属与晶体管电极的通孔,浮栅晶体管单元在黑色区域下方.

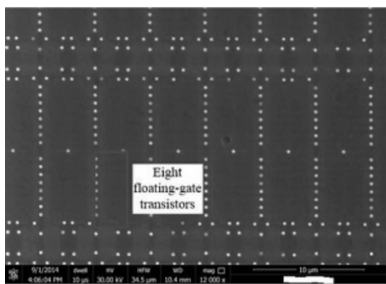


图 10 存储不同内容的相邻数据页对比

因为需要对存储不同内容的晶体管单元进行针对性观测,所以目前状态不符合要求.进一步减薄浮栅晶体管上方的氧化层之后,得到了能够观察到浮栅晶体管的样片,从图中可以清晰看到最小存储器区域中的 8 个浮栅晶体管,如图 11,图 12 所示.

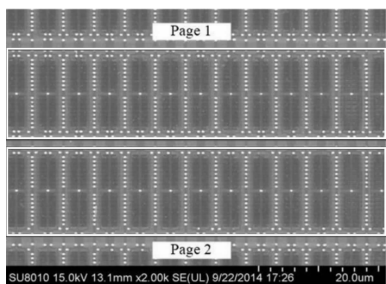


图 11 存储不同内容的相邻数据页对比

按照之前的假设,两个紧邻数据页的数据是不

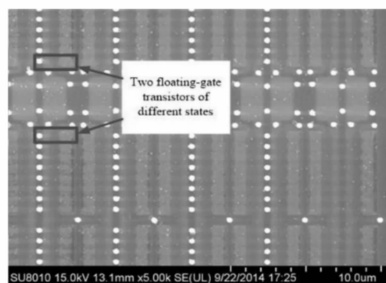


图 12 存储不同内容的浮栅管对比

同的,因此预计有可能会在两个紧邻数据页上发现图像差异,另外直接观察存储不同数据的浮栅晶体管单元也有可能观察出不同,结果分别如图 11 和图 12.结果显示,从图中无法观察出明显的图像差异.因此使用这种方法直接提取 EEPROM 内容难度较大,但是收获是这种方法可以不破坏 EEPROM 单元地定位单个浮栅晶体管单元,弥补了逆向分析的劣势,有一定应用前景.

无法直接读出内容的原因有两个:第一,因为面临破坏浮栅结构的危险,无法继续减薄浮栅管上方的氧化层厚度,导致电子束不能作用到浮栅,从而无法获取浮栅电子信息;第二,依靠不同数量浮栅电子和电子束作用得到的二次电子差别来区分不同存储状态从机理上难度过高.

在实验二的测试过程中,发现测试时把 EEPROM 阵列与周围电路进行电学剥离效果更好,否则将会受到很大的环境噪声的影响.

在制作 PAD 时通常有一些负面影响,因为 PAD 制作需要加高压和大电流,往往会对非易失性存储器内容产生影响.实验过程中,发现对目标存储器电极制作 PAD 后会导致内容发生擦除.

在存储器单元被擦除后测试一次 I-V 曲线;人为按照表 1 参数对存储器单元进行编程之后再读取该单元得到第二条 I-V 曲线.两者的结果比对如图 13 所示,可以看出区别非常明显,因此这种方法经实验验证可行.然而,这种方法的缺点同样存在,主要在于制作 PAD 工程难度大,导致可重复性差,尤其在需要测试较多存储内容时,制作一批 PAD 可能会有较多 PAD 无法工作.

6 结束语

本文实验结果显示,侵入式攻击方法工程难度

(下转第 45 页)

次握手操作后,相连组件开始向以太网设备组件推送数据。第三步当以太网设备组件接收一定的数据后,中断相连组件的传输,将数据传递给底层硬件设备。随后,当以太网设备组件拥有至少一个 MaxPayloadSize 的空间时,它会向相连组件发出恢复数据流信号,数据继续传输。

5 结束语

本文设计的以太网设备组件满足 SCA 规范定义,能够广泛应用于软件无线电台通信组网。在基于 TCP/IP 协议的以太网硬件上实现了有效的封装,为上层波形应用程序和服务提供了统一的以太网接口。在组件内部的数据处理上采用了数据流速控制和发送请求/允许请求控制两类机制,实现了数据的有效传递。本文中以太网设备开发,为 SCA 系统中其他设备组件的开发也提供了参考。

参考文献:

- [1] Magsombol C, Jimenez C, Stephens D R. Joint tactical radio system-application programming interfaces [C] // Military Communications Conference, MILCOM 2007. Orlando, IEEE, 2007: 1-7.

- [2] 范建华,王晓波,李云洲. 基于软件通信体系结构的软件定义无线电系统[J]. 清华大学学报:自然科学版, 2011,51(8):1031-1037.
- [3] JTRS JPEO. Software communications architecture specification, Version 4.0 [EB/OL]. (2001-12-19). [2015-06-11]. <http://jpeojtrs.mil/sca/Pages/portabilityguidelines.aspx>, 2012.
- [4] 邓伟,王玲,施峻武. DSP 上 SCA 波形组件接口的实现[J]. 世界科技研究与发展, 2012, 34(3): 423-426.
- [5] 顾霞萍,赵伟,王宜怀,等. 无线传感网络与以太网无缝结合的应用研究[J]. 微电子学与计算机, 2011, 28(6): 79-83.
- [6] 汤宏萍,王竹平. 嵌入式 TCP/IP 协议栈的设计与实现[J]. 微电子学与计算机, 2008, 25(6): 168-170.

作者简介:

李兰花 女,(1989-),硕士研究生. 研究方向为软件无线电. E-mail:lilanhuayx@163.com.

王玲 女,(1962-),教授,博士生导师. 研究方向为现代网络与通信技术、信息安全、非线性电路与系统.

施峻武 男,(1977-),博士研究生,讲师. 研究方向为软件无线电.

雷鹏斌 男,(1990-),硕士研究生. 研究方向为软件无线电.

黄子鸿 男,(1990-),硕士研究生. 研究方向为软件无线电.

(上接第 40 页)

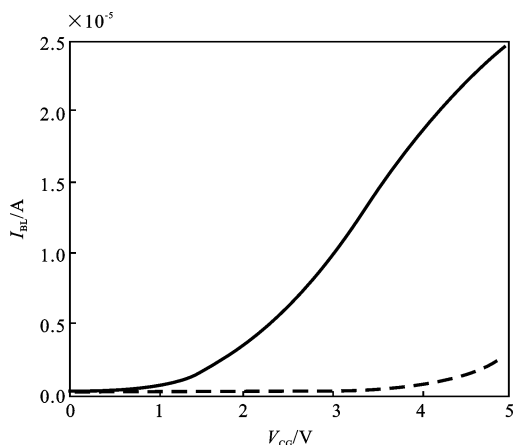


图 13 探针测试结果

大,需要经验积累,但是攻击方式直接,对安全有很大威胁,并且可以和失效分析等仪器和方法相结合,有很多值得研究的切入点。

实验一的探测方法可以明显观测 EEPROM 中单个浮栅晶体管的位置与结构,从而省去某些情况下需要对芯片进行完整逆向分析的繁琐步骤;第二个探针探测攻击方法虽然对 PAD 制作要求高,但是探测少量信息时效果明显。

参考文献:

- [1] Skorobogatov S. Flash memory bumping attacks [C] // International Conference on Cryptographic Hardware & Embedded Systems. Berlin, Springer-Verlag, 2010:158-172.
- [2] Skorobogatov S P. Semi-invasive attacks: a new approach to hardware security analysis [D]. Cambridge, UK: University of Cambridge, 2005.
- [3] Samyde D, Skorobogatov S, Anderson R, et al. On a new way to read data from memory [C] // IEEE Security in Storage Workshop. USA, Maryland, IEEE, 2002:65-69.
- [4] Brown D W, Brewer J E. Nonvolatile semiconductor memory technology: A comprehensive guide to understanding and using NVSM devices [M]. USA, Hoboken: Wiley IEEE Press, 1997.

作者简介:

程鹏 男,(1990-),硕士研究生. 研究方向为针对非易失性存储器的物理攻击技术.

E-mail:chengp12@mails.tsinghua.edu.cn.

白国强 男,(1963-),博士,副教授. 研究方向为应用数学、编码密码学和密码算法的芯片集成技术.