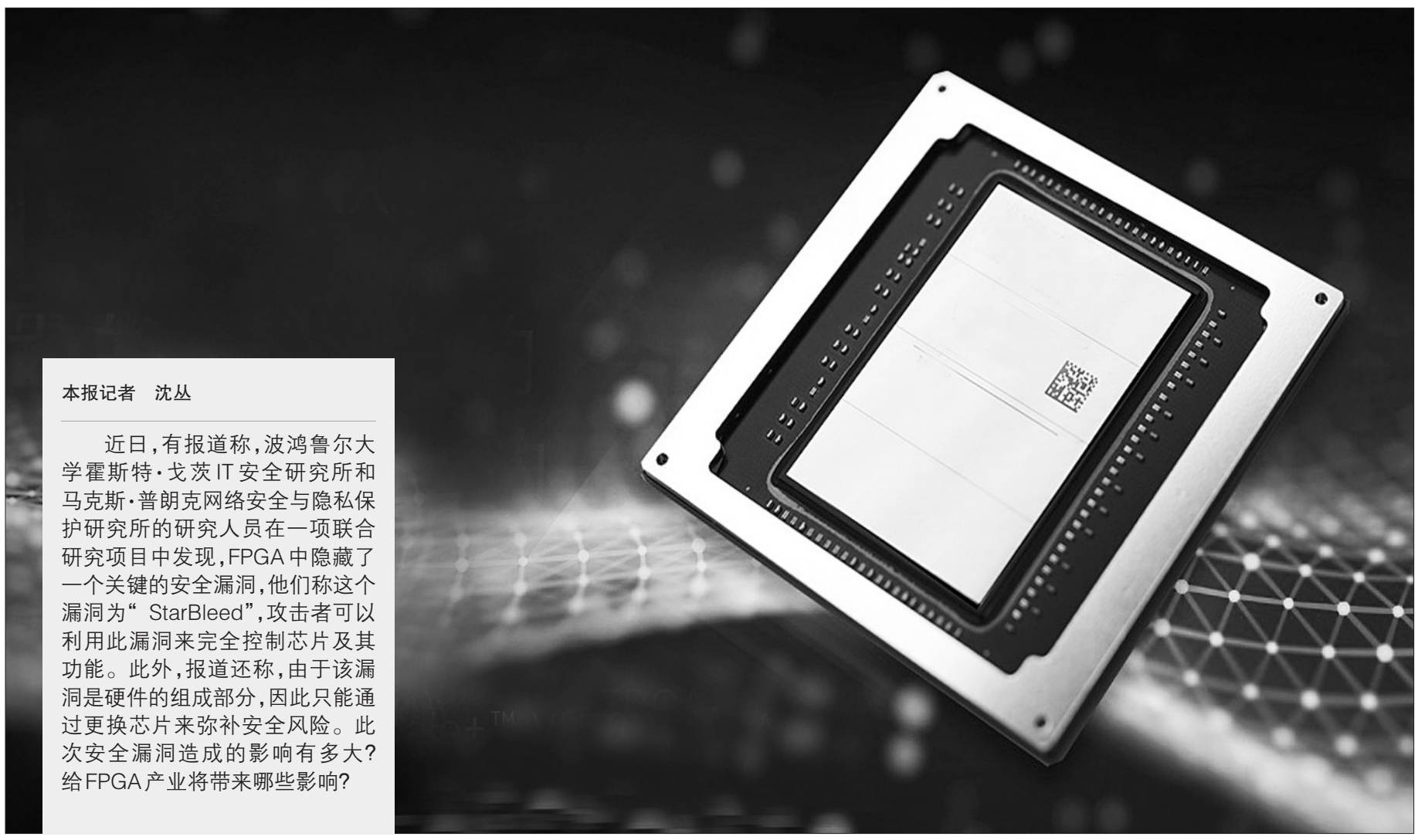
FPGA隐藏了一个安全漏洞？



本报记者 沈丛

近日，有报道称，波鸿鲁尔大学霍斯特·戈茨IT安全研究所和马克斯·普朗克网络安全与隐私保护研究所的研究人员在一项联合研究项目中发现，FPGA中隐藏了一个关键的安全漏洞，他们称这个漏洞为“ StarBleed”，攻击者可以利用此漏洞来完全控制芯片及其功能。此外，报道还称，由于该漏洞是硬件的组成部分，因此只能通过更换芯片来弥补安全风险。此次安全漏洞造成的影响有多大？给FPGA产业将带来哪些影响？

StarBleed是如何形成的

此次安全漏洞正是由于FPGA具有“万能”性，是一种开放、灵活性强的芯片，安全漏洞也会比较多。

山东师范大学物理与电子科学学院讲师孙建辉向记者介绍，FPGA(field-program-gate-array)芯片，有人称之为万能芯片，它具有数字逻辑电路硬件可编程能力，应用场景涵盖军工、民用、工业等。这些应用既可以利用FPGA芯片进行快速逻辑实现，也可以重构为多媒体信息处理编解码芯片，比如多媒体SOC芯片编解码器CODEC、无线通信的基带。

在很多人看来，此次StarBleed安全漏洞正是由于FPGA的这种“万能”性，开放、灵活性强的芯片，安全漏洞也会比较多。赛灵思官网针对这个事件分析，此次研究人员研究的对象，是基于十年甚至十多年前的赛灵思6系列和7系列FPGA器件，攻击者会利用两款器件在AES-CBC模式下缺少误差扩展，同时以WBSTAR为代表的配置命令又可在认证成功前执行，使其得以成功突破器件安全屏障。

若是从硬件方面进行漏洞的修复，往往所耗费的时间和精力都会比较多。

影响究竟有多大

由于FPGA的用途广泛，尤其是在军工、航天和工控这类安全性要求很高的产业需求量很大。此外，这次安全漏洞是发生在硬件的组成部分，比起软件来说修补周期较大，这些是造成此次StarBleed安全漏洞事件引起不小风波的原因。

京微齐力创始人&CEO王海力表示：“修补安全漏洞问题，一般可采用两种方法，从软件修补或者硬件修复下手。从软件下手修补相比较而言周期短、速度快、花费低。例如若是A算法被破译了，就换成B算法加密，现在FPGA针对生成的配置码流采用比较多的是AES256位加密。一般而言，这种算法是比较难以破解的。同时，如果配置码流被破解了，还可以进行软件升级完成补丁修改，总的来说更容易解决一些。”

然而，若是从硬件方面修复漏洞，往往所耗费的时间和精力都会比较多。“一般来说，在硬件方面修复漏洞，需要在硬件电路里面做一些特别的功能，去判断一些恶意攻击的行为，防止别人破解位流，或者监测不按照原有的行为来进行工作的预判电路。这些花费都会很高，因为往往需要重新设计芯片、重新流片并且重新生产。此次研究学者没有特别详细公开关键安全漏洞的机制，从侧面印证了这次StarBleed安全漏洞事件造成了较大影响，因为这个安全漏洞有可能是出在了硬件的组成部分。”王海力说道。

赛灵思发言人向记者表示：“这次安全事件出来之后，美国总部第一时间给了设计建议来规避这个安全隐患。而且这次漏洞虽然在硬件上，但是若想通过这个漏洞来进行攻击也并不是件容易的事情，需要有一个前提条件，那就是必须是物理上可以近距离接触到这个硬件。也就是说，其一，若想进行攻击，必须有近距离的物理接触，但是这并不容易实现；其二，若想实现远程攻击，需要在接口设置为外部可以访问的情况下才可实现，如果接口不设置外部访问，就不会出现这个问题。”

在一些应用领域，采用国密算法来加密，不易被破解，安全性能更高。

巧妙利用变“废”为宝

在王海力看来，此次攻击者利用的手法其实并不是新型的手段：“早在十年前，黑客就会利用控制配置码流的技术来入侵。这么多年过去了，FPGA的安全性能在不断提升，黑客技术也在不断提升。一般来说，开放、灵活性强的芯片，安全漏洞也会比较多。这往往是相伴而生的，黑客问题肯定是无法完全避免，但正是因为有黑客的存在，也使FPGA需要不断更新迭代、修补漏洞。从某种意义上讲，这也促进了FPGA技术的发展。”

孙建辉认为，这次安全漏洞事件虽然向所有FPGA研发单位敲了一次警钟，但同时也可以反向利用这次安全漏洞，变“废”为宝。“比如我们可以基于远程无线操纵码流存储体，远程重构更新逻辑功能，并且若用户具有私有权限，甚至可以设置权限，进行授权访问码流修改权限，而恶意入侵者却被严密的安全防护网络阻挡在门外，这无疑是一件因祸得福的事情，也会促进国际FPGA硬件重构芯片的发展，以及推出新的标准或新的研发规范。”孙建辉说。

王海力表示，虽然比起国外FPGA来说，国内FPGA起步较晚，技术较为落后，但是中国还是有自己的优势的。在安全性能上，国产FPGA可以做一些自己的特色，比如在加密算法中，在一些应用领域，采用国密算法来加密，不易被破解，安全性能更高。此外，国产FPGA可以借鉴很多国外PFGA的发展经验，避开很多雷区，使国产FPGA在安全性能上能够发展得更快更好。

同时，孙建辉认为，这次StarBleed安全漏洞事件也给了国产FPGA一定的反思，让国产FPGA企业能够思考如何设计FPGA万能芯片，用什么全新的物理、电路、算法以及配置下载流程技术能够进行安全性更高的FPGA重构设计？国内企业等单位如果抓住机遇，推出最新的安全FPGA芯片，拥有国际专利、推出新标准，这无疑是一次突围的好机会。

2021年NAND Flash市场竞争加剧

本报讯 根据集邦咨询半导体研究中心（DRAMeXchange）调查，长江存储（YMTC）已在第一季度将128层3D NAND样品送交存储控制器厂商，目标是第三季度进入投片、年底前量产，拟用于UFS、SSD等各类终端产品，并同时出货给模组厂。考虑到客户导入的时间，预估长江存储新产品可能率先影响第四季度Wafer市场合约价，并自2021年起对Client SSD、eMMC/UFS等市场供给产生实质贡献，在供给增加的情况下，价格下跌的可能性也将提高。

集邦咨询表示，受到疫情影响，智能手机及笔记本电脑等终端需求将受到不小冲击，并对NAND Flash主流供应商获利能力造成影响，抑制未来持续扩产的幅度。相较之下，长江存储目前在各类应用的市占规模仍小，因此受疫情影响较低。当前目标将着重于与OEM进行64层TLC的相关产品导入及提升良率，并赶在今年内送交128层产品样品，将同时包含TLC以及QLC产品，以扩大客户基础。

3D NAND堆栈难度渐增，有利长江存储缩小差距。随着3D NAND Flash堆栈达到90层以上，主要供应商在更高层数蚀刻及堆栈技术的发展难度逐渐增加。观察各供应商的技术路线图，在1XX层的产品世代已有分歧：尽管三星、SK海力士已推出128层产品，但铠侠/西数、美光、英特尔的112/128/144层产品要到下半年才会放量，相比前几代3D NAND产品的发展进程更久，有利于长江存储的128层产品迎头赶上。

除此之外，2019年NAND Flash的价格平均跌幅达46%，导致主要供应商陷入亏损，资本支出因而转为保守，产出增长规划亦创下历史新低，这也让长江存储有了拉近差距的机会。

2021年长江存储产能预估占整体NAND Flash约8%。身为新进供应商的长江存储目前拥有武汉厂，今年目标是成都厂开始投产，并逐步完成武汉厂区剩余二座厂房的兴建与扩产。预期NAND Flash市场竞争将加剧，长期价格面临持续下跌的压力。（集邦咨询）

日前，上海韦尔半导体股份有限公司公告称，将通过现金增资方式收购Synaptics公司亚洲地区的TDDI业务，交易总价格1.2亿美元。TDDI的市场有多大？未来的发展前景如何？

韦尔开启国际收购 TDDI市场前景如何？

本报记者 陈炳欣

产值10亿美元且市场仍在成长

TDDI即整合显示驱动IC和触控IC的集成芯片。随着显示技术的不断发展，触控显示装置得以广泛应用，TDDI芯片将面板驱动IC和触控面板IC集合到一颗芯片当中，可以有效提高触控显示装置的集成度，使移动电子设备更轻薄、成本更低、显示效果更好。

Synaptics公司于2015年率先推出两款TDDI解决方案ClearPad 4191和Clear Pad 4291，受到行业认可。经过最近几年的发展，TDDI技术逐渐成为智能手机等移动终端显示及触控领域的主流技术之一。根据CINNO Research统计数据，2019年全球TDDI驱动芯片出货规模超7亿颗，产值在10亿美元左右。

CINNO Research首席分析师周华分析指出，目前智能手机市场主流技术为AMOLED、LTPS LCD和a-Si LCD。TDDI技术主要搭配在LTPS LCD上，在AMOLED上短期内无法实现触控显示一体化驱动，且必要性不如LCD面板。a-Si目前使用TDDI技术的渗透率非常低，且并非未来主流趋势。随着未来智能手机市场上AMOLED渗透率快速提升，将明显挤占LCD市场，短期内LTPS LCD还可以进一步挤占a-Si LCD的市场维持其市场份额，中长期来看势必会受到影响，市场份额将逐步降低，同时考虑到TDDI芯片价格的持续走低，CINNO Research认为TDDI市场至2021年仍将继续上升，2022年开始市场规模会逐步下降。

此外，中国台湾地区显示芯片大厂联咏总经理王守仁认为，部分低阶智能手机及过去采用分离式解决方案的机型2020年会转而采用TDDI，比如功能型手机亦将逐渐改为TDDI，这也将极大促进TDDI芯片的出货量。

中国台湾厂商占据市场主导地位

目前的TDDI市场上，中国台湾厂商占据较大优势。2019年，联咏在该领域的市占率相较2018年增长了10%，达到40%的市场份额。相比之下，Synaptics则从2018年的25%下降到15%的份额。这也成为Synaptics选择剥离旗下TDDI芯片业务的主要原因。

根据周华的介绍，目前TDDI业务的主要厂商为中国台湾地区厂商，包括联咏科技、敦泰科技等。现在中国大陆厂商也投入这一领域积极发展。除韦尔半导体通过收购进入该市场外，此前集创北方与晶门科技均推出相关产品。

集创北方推出的触控显示驱动单芯片方案ICNL9911，支持面板减光罩方案，并减少下边框400μm~500μm，具有卓越的显示、触控性能，实现了1+1>2的效果，性能较分立式方案有了显著提升，能够更好地支持全面屏设计。晶门科技TDDI芯片SSD2092获得HTC智能手机U12 Life所选用，该产品在柏林IFA（国际电子消费品展览会）2018上发布。

有专家指出，通过上下游的产业互动，将会有效带动本土显示IC在技术上的提高。因为品牌厂商面对客户，对于市场需求有着更加到位的掌握，他们可以提出需求，有利于显示IC厂商进行产品的定义与开发。通过这些具有差异化的产品，中国大陆本土厂商有机会追赶国际厂商。

TDDI在AMOLED面板中试水应用

从TDDI的技术趋势上看，LCD的驱动芯片技术已经非常成熟，未来还是持续在低功耗、低成本方面做努力。目前，芯片厂商们在TDDI芯片的量产上正在从80纳米陆续向55纳米转变。集邦咨询研究协理范博毓指出，IC厂商开始将TDDI的生产从集中在80纳米节点，改为向不同晶圆厂的55纳米节点移转。

此外，2020年随着越来越多5G网络服务在各个区域陆续展开运营，更多手机品牌厂商把高刷新率（90Hz以上）面板作为实现产品差异化的重点，IC厂商也开始在55纳米节点重新打造90Hz/120Hz用的TDDI IC，全力在传统TFT-LCD机种上推升新的需求。

TDDI在AMOLED面板的应用也是今后的一个观察点。虽然目前AMOLED采用TDDI的动力不足，这与AMOLED主要采用On-cell技术制造有关，使用TDDI并不会大幅降低面板成本。但有消息称，三星Galaxy Note 10+ 5G的super AMOLED屏幕上就采用了TDDI技术。苹果也有望在今年的某款手机AMOLED屏幕上试水TDDI。这些举动均有可能推动TDDI在AMOLED市场的发展。

社长：张立 社址：北京市海淀区紫竹院路66号赛迪大厦18层 邮编：100048 每周二、五出版 周二8版 周五8版 零售4.50元 全年定价420元（包含手机客户端） 广告部：010-88558848/8808 发行部：010-88558777 京昌工商广登字第20170004号 经济日报印刷厂印刷