一种新型自毁芯片监测和执行电路的设计

胡长征，马　伟，高清运，胡伟波
（南开大学 电子信息与光学工程学院，天津 300350）

摘　要： 针对当前自毁技术中，自毁监测方式单一且自毁执行较长和自毁不彻底、不稳定导致自毁成功率较低的问题，设计了一种同时具备自毁实时监测和执行的电路系统。该电路系统设计了封装拆卸和上电时序两种自毁监测方式，使自毁监测的方式更加多样，提高结果的准确性。同时利用 MOS 管作为开关特性，来减少自毁执行的时间。实验结果表明，该电路系统在 3.3 V 的供电电压且钽电容存储电压为20 V 时，可以通过自毁监测电路对工作芯片进行实时的监测，同时经过测试表明，从监测到自毁信号到自毁执行开始，需要时间为 0.28 ms。

关键词： 自毁芯片；实时自毁监测；自毁行
中图分类号： TN409　　**文献标识码：** A　　DOI：10.16157/j.issn.0258-7998.211819

中文引用格式： 胡长征，马伟，高清运，等. 一种新型自毁芯片监测和执行电路的设计[J]. 电子技术应用，2022，48(2)：23-27.
英文引用格式： Hu Changzheng，Ma Wei，Gao Qingyun，et al. Design of a new type of self-destruct chip monitoring and execution circuit[J]. Application of Electronic Technique，2022，48(2)：23-27.

Design of a new type of self-destruct chip monitoring and execution circuit

Hu Changzheng，Ma Wei，Gao Qingyun，Hu Weibo
（College of Electronic Information and Optical Engineering，Nankai University，Tianjin 300350，China）

Abstract： In the current self-destruction technology，the self-destruction monitoring method is single，the self-destruction execution is long，and the self-destruction is incomplete and unstable，which leads to the low success rate of self-destruction. A real-time monitoring and execution circuit system with both self-destruction monitoring and execution is designed. The circuit system designed two self-destruct monitoring methods，packaging and disassembly and power-on timing，which made the self-destruct monitoring methods more diverse and the results more accurate. At the same time，MOS tube was used as the switching characteristic to reduce the time of self-destruct execution. The experimental results show that the circuit system can carry out real-time monitoring of the working chip through the self-destruct monitoring circuit when the supply voltage is 3.3 V and the storage voltage of tantalum capacitor is 20 V. Meanwhile，the test results show that the time from the monitoring to the self-destruct signal to the start of the self-destruct execution is 0.28 ms.

Key words： self-destruction chip；real-time self-destruction monitoring；self-destruction execution

0 引言

当前自毁技术应用广泛，在无人机的侦察系统、机密数据的存储设备[1]以及关键芯片、电子政务和金融等领域都有很好的应用[2]。2016 年，Jin-Woo Han 等人提出了一种自毁式鳍片触发器驱动的晶体管，在需要芯片自毁时，向触发栅极施加触发电压，产生的静电弯曲应力将破坏鳍片的源-漏延伸区域，使晶体管断开，电路失去原本功能。2017 年，解放军海军医学研究所提出一种新的自触发方法，这种方法是在监测电路感知到设备外壳上的螺丝被拧下时[3]，产生高电流信号使芯片烧毁。2018 年长春闻鼓通信公司通过控制端发出自毁命令[4]时，芯片保护电路内部产生高压击毁芯片，以此达到防止信息泄露的目的。

在大多数自毁设计和应用中，自毁监测的方式一直被忽视，导致自毁监测方式单一，准确灵敏性较低。同时在监测到自毁状态到产生自毁信号，开始执行自毁的整个过程时间较长，且其自毁程度不够彻底，有时只能停止电路的正常工作，不能真正地破坏芯片数据的存储模块。

本设计针对自毁监测方式和自毁信号产生速度的问题，基于阈值判断等算法[5]，提出了一种新型自毁芯片监测和执行电路系统，可以通过封装拆卸和上电时序[6]，对芯片工作环境进行监测，同时利用阈值判断等算法对监测数据进行分析和处理，产生自毁执行信号，在较短的时间内执行自毁。

1 自毁监测系统原理和硬件电路设计

1.1 自毁封装监测电路原理

传统自毁系统中的自毁监测电路的设计都存在一

定的缺陷，监测方式单一、不能对被保护芯片实现真正的实时监测、同时对监测到的数据不能进行客观和准确的判断以至于产生漏判和错判的失误情况[7]，造成额外的损失。

针对以上自毁电路设计的缺陷，本文研究设计了一种新型的自毁检测电路。该电路主要是根据芯片封装层金属网与芯片内部电路地之间的定值电阻(简称“内阻”)进行检测的[8]，如图 1 所示。

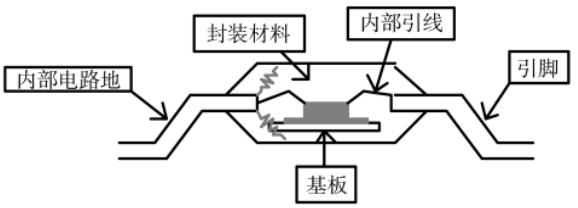

图 1　芯片内阻连接示意图

因此，根据这一特征，利用特殊工艺将一个阻值远远大于封装完好时内阻阻值的外接电阻连接到芯片封装层的金属网，外接电阻的另一端连接到系统电源 VCC，芯片内阻与外接电阻构成串联-分压电路，通过检测内阻和外接电阻之间的模拟电压值，就可判断出当前芯片的封装和自身工作的情况。

1.2 自毁封装监测硬件电路设计

依据自毁封装监测电路的原理，进行对应的电路设计，如图 2 所示。

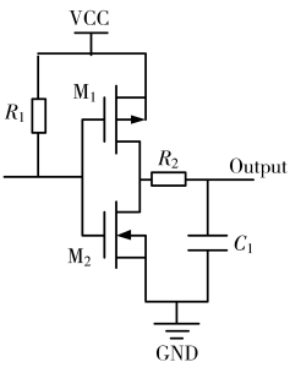

图 2　封装监测电路概念图

图中 R_1 为封装的外接电阻，一般阻值设为 1 MΩ 到 10 MΩ 之间。图中 M1 和 M2 组成取反电路可以将输入的模拟电压进行取反。由于芯片内阻阻值存在偏差范围，故其所产生的模拟电压值也会存在变动。自毁指令启动模块检测到的芯片数据和真实值会存在偏差，导致数据处理结果和指令发生错误。

1.3 上电时序监测原理

本设计针对被保护芯片自毁监测方式单一的缺陷，研究设计一个新型的自毁监测方式——上电时序监测[9]。常规芯片的上电是芯片电源端的电压从零伏转变为芯片所需的额定电源电压，之后便由系统电源持续为芯片提供额定电源电压，保持不变。本设计针对这一个简单的上电时序进行改变，设定特定的上电时序，如图 3 所示。上电时序为：先上电，维持时序按 T，断电，维持时间 T_1，再次上电，其中 T 和 T_1 大于零且可以单独设定。

1.4 上电时序监测硬件电路实现

上电时序监测模块电路实现由一个控制芯片电源电压的单刀双掷开关和稳压滤波的电容组成，如图 4 所示。S1 开关下拨时，监测芯片停止工作；上拉时，监测芯片开始正常工作。在开关上拨下拉时，电压 Output 端的电压会经过二极管 D1 并发生改变。改变的电压会被自毁指令模块监测到，并进行数据分析。

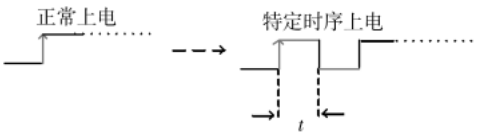

图 3　上电时序对比示意图

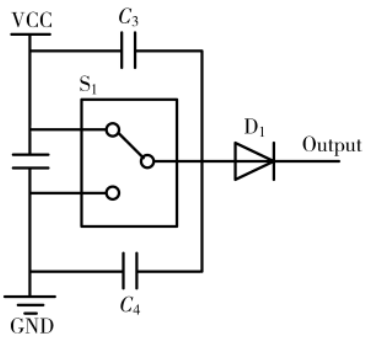

图 4　上电时序监测模块示意图

2 自毁执行系统原理和硬件电路设计

2.1 自毁执行模块原理

针对上面所述自毁执行方法的缺陷，本设计提出一种新型芯片自毁的方式，利用超级电容存储大量电荷，在接收到自毁指令[10]信号时，会快速将电荷释点燃由 Al 和 Ni 溅射而成的纳米高能膜，进而破坏芯片内部数据存储结构。利用特殊工艺，将超级电容的两端并联到高能膜的表面同一侧。遇到突发状况时，存储着大量电荷的超级电容与高能膜连接导通，且高能膜表面的阻抗较小，高能膜表面会在瞬间产生很高的热量，进而点燃高能膜，烧毁芯片。

2.2 自毁执行模块硬件电路设计

自毁执行模块采用体积小、容量大的钽电容和由 NMOS 和 PMOS 组合的开关电路连接构成，可以降低延迟时间，增强自毁强度。自毁执行模块接收到自毁指令信号，首先经过 NMOS 和 PMOS 组成的开关电路，如图 5 所示。

正常情况下，指令信号为高，PMOS 闭合，NMOS 断开，超级电容与高能膜断开，超级电容处于充电状态；危险情况时，指令信号由高电平变为低电平，PMOS 断开，NMOS 闭合，超级电容连接高能膜，超级电容开始放电。高能膜表面会瞬间产生很大的热量[11]，烧毁芯片内部存储数据的电路[12]，自毁执行模块电路如图 6 所示。

3 自毁电路综合测试结果

基于上述关于自毁芯片的原理分析和电路设计的介绍，完成了自毁芯片综合系统的焊接和功能的测试。自毁芯片综合系统板如图 7 所示。

3.1 自毁监测端测试

自毁监测端测试主要包括：封装自毁监测和自毁执

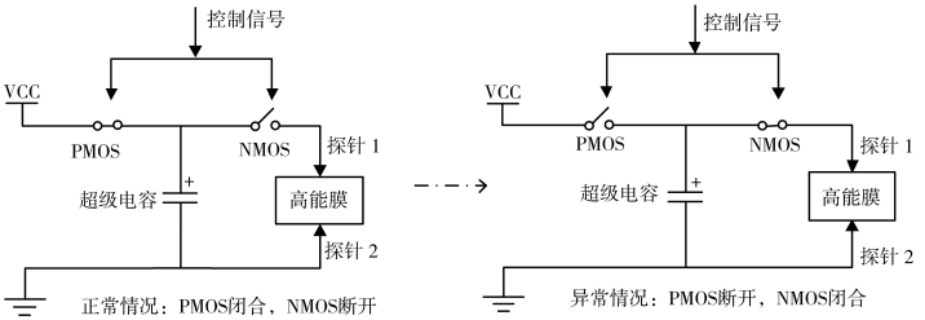

图 5　NMOS 和 PMOS 组成的开关示意图

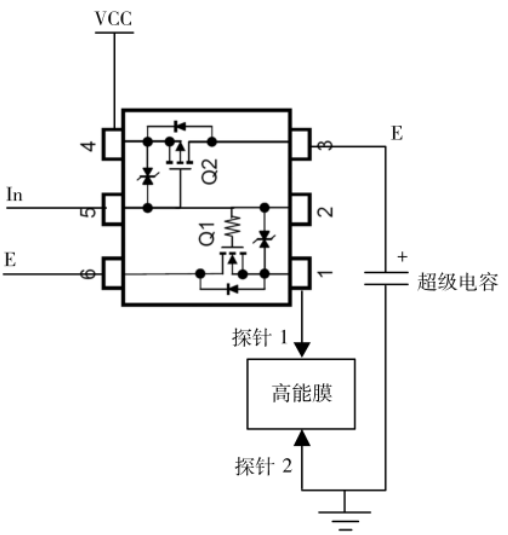

图 6　自毁执行电路

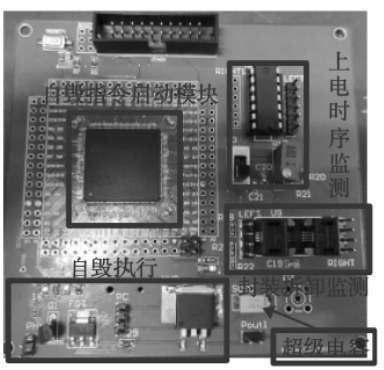

图 7　自毁监测综合版

行端测试。依据上述封装自毁监测的原理，完成自毁封装监测端的测试，测试结果如图 8 所示。正常状态下，封装未遭到破坏，芯片工作状态指示灯保持点亮状态。异常状态时，封装遭到破坏，同时芯片工作状态指示灯熄灭，表示芯片已经监测自毁状态，产生自毁信号。

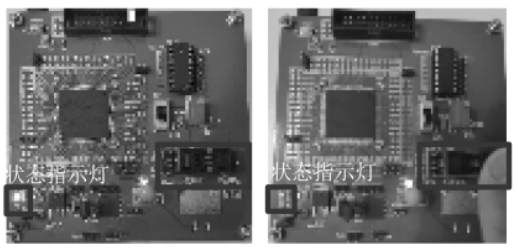

图 8　自毁封装监测板级电路(图左为正常状态，图右为异常状态)

3.2 自毁执行端测试

自毁点燃测试过程主要利用千眼狼 X213 高速摄像机来记录当自毁执行信号传输到自毁执行模块，高能膜的点燃和燃烧的过程。千眼狼 X213 是一款超高速万帧级别的超大内存高速摄像机，其最大分辨率可达到 1 280×1 024，满幅采集速度可以达到 12 400 fps，故其完全可以达到测试高能膜自毁全过程。基于上述自毁执行端测试原理，当自毁执行信号到来后超级电容开始放电，高能膜被点燃。高能膜燃烧的整体过程如图 9~图 11 所示。

经过实际测试表明，利用电容存储的能量完全可以

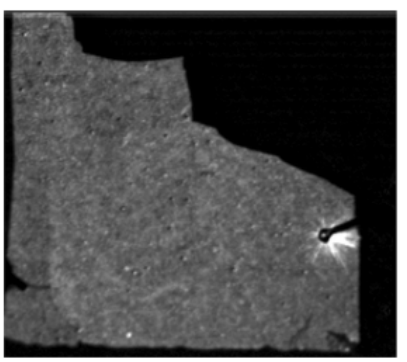

图 9　高能膜开始点燃

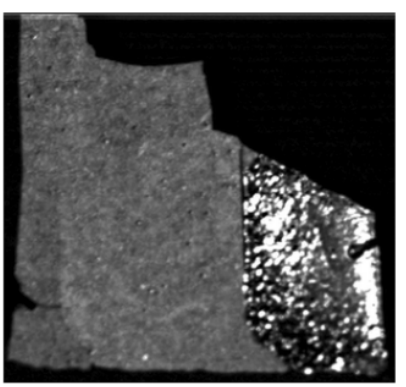

图 10　高能膜点燃中

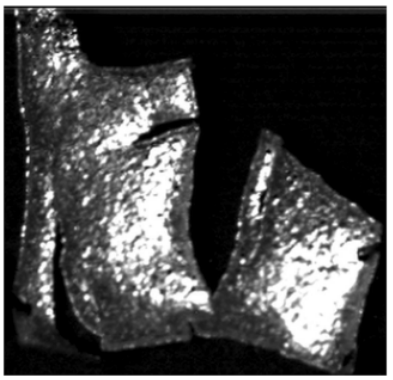

图 11　高能膜点燃完成

将高能膜快速点燃，进而利用高能膜燃烧释放的能量，来破坏芯片的内部结构，达到芯片自毁，保护机密数据目的。

3.3 自毁延迟时间测试

自毁芯片单元从监测到自毁信号到点燃高能膜的延迟时间主要包括三部分：监测模块监测到异常情况到自毁信号的产生、自毁执行模块接收到自毁指令信号到高能膜被点燃以及电信号在 PCB(印刷电路板)导线中传输的时间。

3.3.1 电信号在 PCB 中传输时间

信号在媒质中传播时，其传播时间主要由信号载体和周围媒质属性所决定。电信号在真空中传输的速度为 3×10^8 m/s 或 11.8 inch/ns。在其他介质中，相对介电常数为 E_r，则其传播速率为 $\frac{11.8}{\sqrt{E_r}}$ inch/ns，本实验所使用的 PCB 是一般的 FR4 板材，其介电常数约为 4.6，所以信号在 PCB 中传播的速率是5.5 inch/ns，则其传播时延约为 0.18 ns/inch，经计算从自毁检测端到自毁执行端信号导线共长 9 000 mil 即 9 inch，故自毁信号在 PCB 中传输过程中的时延为 1.62 ns 即 1.62×10^{-6} ms。

3.3.2 监测模块监测到异常状态至自毁信号的产生

自毁指令启动模块接收到自毁监测端传输的信号后，经模数转换将模拟信号转换为数字信号，并通过阈值分析判断等算法对数据进行处理，最后由自毁启动模块根据算法分析的结果，产生对应的指令信号。信号的整体处理过程都在自毁启动模块中，而模块处理数据的时间则取决于该模块系统的机器周期和时钟频率。本实验中自毁指令启动模块外接 12 MHz 晶振作为时钟来源，其每执行一条指令所需时间为 1 μs，经计算自毁指令启动模块的指令执行和逻辑延时共需 100 μs 则监测模块监测到异常状态至自毁信号的产生共需要 100 μs。

3.3.3 自毁执行模块接收到自毁指令信号到高能膜被点燃

由自毁执行模块的工作原理和工作过程可知，实验中自毁执行端是利用超级电容可瞬间放电的特性产生大量热量来点燃高能膜，烧毁芯片。因此，本阶段的所需时间可以通过电容的放电时间进行估算：

$$V_t=V_0+(V_1-V_0)\times[1-e^{-\frac{t}{RC}}] \tag{1}$$

$$t=RC\times\ln^{\left[\frac{V_1-V_0}{V_1-V_t}\right]} \tag{2}$$

其中，V_0 为电容上初始电压，V_1 为电容最终可充到或放到的电压值，V_t 为 t 时刻电容上的电压。实验中超级电容的电压最高可达到 30 V，电容开始放电。由电容特性和公式可知，电容放电过程中最终的电压值会无限地趋近于 0 V，但不会达到 0 V。且在本实验中，高能膜在电容放电的前期就可以点燃高能膜。若假设最终放电的电压为 0.1 V，则此时的时间 t 肯定大于自毁执行模块从接收自毁指令信号到点燃高能膜的时间延迟。则 V_0=30 V，V_1=0 V，V_t=0.1 V，经计算可得 t=0.27 ms，由此可知自毁执行模块从接收到自毁指令信号到点燃高能膜所需时间的最大极限值为 0.27 ms。

综上可知，电信号在 PCB 中传输所消耗的延时为 1.62×10^{-6} ns，可以忽略不计，故自毁芯片单元从监测到芯片的自毁状态到点燃高能膜，所需最长时间为 0.37 ms< 1 ms，可以大大增强芯片的安全性。

3.3.4 实际测试结果

本实验利用示波器 Trigger 的触发检测边沿的和短时间脉冲的功能，来测量检测自毁芯片单元自毁延迟时间。在系统电路外部外接信号处理电路——异或门，开始状态，自毁监测触发端和自毁执行端的信号都为低电平，监测到异常状态，自毁监测触发端的信号变高，自毁执行端的信号依然为低，此时异或门则会产生高脉冲，直到信号处理后自毁执行端的信号也变为高电平，开始执行自毁时，异或门会再次输出低电平，中间的高电平脉冲时间即为信号传输延迟时间。设置好示波器的 Trigger 功能后，将示波器的探头与自毁芯片综合版对应管脚连接好后，开始测试，测试结果如图 12 所示。

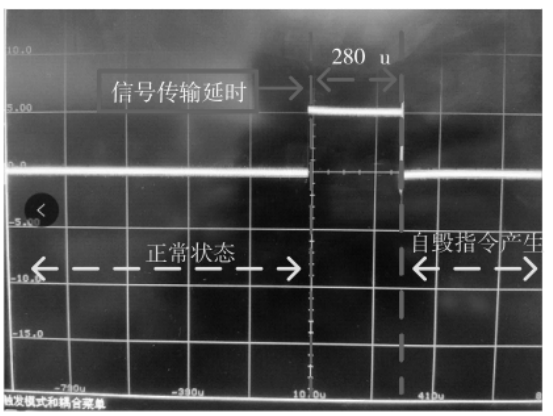

图 12　示波器 Trigger 捕捉波形

根据自毁芯片综合版和示波器联合测试的结果可知，自毁芯片单元自毁延迟的时间为 0.28 ms<1 ms。

4 结论

本文研究设计了一种新型自毁监测和自毁执行系统电路。新型自毁监测电路包括封装拆卸监测电路和上电时序监测电路，可以对被保护芯片进行实时保护监测，电路简易，功耗低。新型自毁执行电路利用超级电容和高能膜构成，在断电的情况下，自毁执行系统依然可以执行自毁，保护芯片内部存储的信息。自毁监测和执行系统的自毁延时可以小于 1 ms，实现了实时监测、快速自毁的低功耗自毁监测和执行。

参考文献

[1] 王帅，高秀峰，李玺，等.涉密 U 盘自毁装置：CN 204657084 U[P].2015-09-23.

[2] CHRISTOPHER K.This message will self-destruct：the growing role of obscurity and self-destructing data in digital communication[J].Bulletin of the American Society for Information Science and Technology(Online)，2013，40(2).

[3] 赵玉清，孙良成，李建强，等.集束子弹药引信独立自毁自失效设计方法[J].兵器装备工程学报，2018，39(12)：41-45.

[4] KIM Y K，HONG C S.Threshold estimation in self-destructing scheme using regression analysis[C]//2017 19th Asia-Pacific Network Operations and Management Symposium(APNOMS)，2017：135-138.

[5] Self-destructing silicon chip[J].Materials Today，2002，5(3).

[6] 姜冬，王慧强，冯光升，等.基于模糊层次化评估的分布式系统自毁感知方法及应用[J].小型微型计算机系统，2012(4).

[7] CAO Q，CHENG K，LI Z，et al.Prevention of reverse engineering of security chips：U.S.Patent 9，853，001[P].2017-12-26.

[8] FU X，WANG Z，WU H，et al.How to send a self-destructing email：a method of self-destructing email system[C]//2014 IEEE International Congress on Big Data，2014：304-309.

[9] 衡立业.数据加密和异常数据自毁技术在网络信息安全中的研究[J].网络安全技术与应用，2020(6)：35-36.

[10] GU X，LOU W，SONG R，et al.Simulation research on a novel micro-fluidic self-destruct device for microchips[C]//2010 IEEE 5th International Conference on Nano/Micro Engineered and Molecular Systems，2010：375-378.

[11] JEFF A，STEVEN T，JEFFREY J.Self-destructing electronic device：U.S.Patent 9812407[P].2017-11-07.

[12] ZENG L，CHEN S，WEI Q，et al.Se Das：a self-destructing data system based on active storage framework[C]//2012 Digest APMRC，2012：1-8.

（收稿日期：2021-05-31）

作者简介：

胡长征(1996-)，男，硕士研究生，主要研究方向：数字集成电路、嵌入式系统等。

马伟(1995-)，男，博士研究生，主要研究方向：模拟射频集成电路设计。

胡伟波(1982-)，通信作者，男，博士，研究员，主要研究方向：模/数和数/模转换器、无线感知芯片和系统实现、第三代半导体、生物芯片，E-mail：weibohu@hotmail.com。

扫码下载电子文档

（上接第 22 页）

[7] 赵雪花，陈旭袁，旭琦.基于 EMD 的数据驱动模型在径流预测中的应用[J].系统工程，2014，32(9)：150-154.

[8] 司友强，吴润华，施鹏程.基于 EMD，EEMD 与 CEEMD 的信号时频分析技术对比研究[J].CT 理论与应用研究，2019，28(4)：417-426.

[9] WU Y，WU Q，ZHU J.Improved EEMD-based crude oil price forecasting using LSTM networks[J].Physical A：Statistical Mechanics and Its Applications，2019，516：114-124.

[10] 李洁，林永峰.基于多时间尺度 RNN 的时序数据预测[J].计算机应用与软件，2018，35(7)：33-37.

[11] YU Y，SI X，HU C，et al.A review of recurrent neural networks：LSTM cells and network architectures[J].Neural Computation，2019，31(1)：1-36.

[12] 超人汪小建.GRU 神经网络[EB/OL].(2017-08-17)[2021-03-16].https://blog.csdn.net/wangyangzhizhou/article/details/77332582.

[13] 陈雯柏，吴细宝，陈启丽.人工神经网络原理与实践[M].西安：西安电子科技大学出版社，2016：44-47.

[14] VASWANI A，SHAZEER N，PARMAR N，et al.Attention is all you need[J].ArXiv：1706.03762，2017.

[15] BAI S，KOLTER J Z，KOLTUN V.An empirical evaluation of generic convolutional and recurrent networks for sequence modeling[J].ArXiv：21803.01271，2018.

（收稿日期：2021-03-16）

作者简介：

徐海兵(1982-)，男，硕士，高级工程师，主要研究方向：时序预测、智能运维、OCR、视频理解。

郭久明(1982-)，男，本科，工程师，主要研究方向：数据通信网络、意图驱动网络。

扫码下载电子文档

版权声明