

UEFI BIOS&APP 编程 开发查询手册

作者：朱工

微信：lahmyyc638

Talk is Cheap!

Show me the Code!

存储行业十余载的宝贵经验总结，全书 100 多个章节，4000 多页，超级硬核！不仅有 DRAM 内存地址编解码源代码的深度剖析、DRAM 和 SSD 测试代码各个子功能深度剖析，还有很多其他方方面面的 UEFI 常用功能的代码实现！更有内存测试算法、SSD FTL 算法设计，全是代码干货！需要很大的耐心！合适作为日常 UEFI 编程查询手册使用！

目录

电子书更新说明	31
序言	33
如何获得该 PDF 电子书?	33
温馨提示	33
警告	34
为什么要整理成书?	34
第 0 章 UEFI BIOS&APP 开发环境搭建	37
0.1 基于 EDKII 的 UEFI APP 编译开发环境搭建	37
0.2 HelloWorld 示例程序的编写	68
0.3 AMI BIOS 的编译开发环境搭建	73
0.4 AMI BIOS 源代码的调试环境搭建	80
0.5 Insyde BIOS 编译开发环境搭建	81
0.6 Byosoft BIOS 编译开发环境搭建	84
第 1 章 UEFI 框架下, 内存测试程序的基本框架	87
1.1 为什么要进行内存测试?	87
1.2 内存测试软件的整体框架	88
1.3 技术实现	90
1.4 BIOS 启动阶段的 DDR 内存测试	102

第 2 章、UEFI 框架下，内存测试程序的背景颜色设定与实现.....	129
第 3 章、UEFI 框架下，键盘事件、菜单功能的代码实现.....	133
3.1 按键功能.....	133
3.2 菜单功能.....	137
第 4 章、UEFI 框架下，CPU ID、Cache 缓存信息的获取与实现	142
第 5 章、UEFI 框架下，获取文件目录和文本文件的读写与实现.....	154
5.1 获取文件目录	154
5.2 文本文件的读写	159
第 6 章、UEFI 框架下，内存条 SPD 数据的读写与实现.....	166
6.1、SMBUS 协议简介	166
6.2、SPD 的介绍	168
6.3、SPD 寄存器	174
6.4、SPD 数据的读写(以 DDR5 为例)	177
6.4.1 Write Operation - Data Packet.....	178
6.4.2 Read Operation - Data Packet.....	181
6.5、代码剖析	184
6.5.1 DDR5 SPD 的解析代码.....	187
6.5.2 DDR4 SPD 的数据解析的代码实现.....	198
6.5.3 DDR3 SPD 的数据解析的代码.....	204

6.5.4 DDR2 SPD 的数据解析的代码.....	211
6.5.5 DDR SPD 的数据解析的代码.....	218
6.5.6 RDRAM SPD 的数据解析的代码.....	222
6.5.7 SDRAM SPD 的数据解析的代码.....	226
6.6、BIOS 对 SPD5 的处理.....	229
6.7、内存条的 SPD 数据的改写.....	232
6.8、笔记本板载内存的 SPD 数据的改写	232
第 7 章、UEFI 框架下，SMBIOS 信息的获取与实现.....	237
第 8 章、UEFI 框架下，网络信息的获取与实现.....	246
8.1、网络框架	246
8.2、代码说明	251
8.3、真实 UEFI 环境下使用网络.....	255
8.4、TCP/UDP 网络编程的实现.....	258
8.4.1 EFI_TCP4_PROTOCOL 的使用.....	258
8.4.2 TCP4 的编程	264
8.4.3 测试.....	281
第 9 章、UEFI 框架下，内存的实时频率和时序的获取与实现.....	283
第 10 章、UEFI 框架下，获取内存映射地址，筛选可分配内存地址，进一步筛选出可 用来测试的内存地址，分配对应内存地址空间给可测试的内存地址	302

第 11 章、UEFI 框架下，获取 CPU 内核数和线程数，BSP 和 AP 核的初始化，装载测试内存地址空间给每个 CPU 核心或者线程.....	304
第 12 章、UEFI 框架下，内存故障类型，测试算法的设计与实现.....	313
12.1 DRAM 的故障模型	313
12.1.1 静态 RAM 故障模型	313
12.1.2 动态 RAM 故障模型	315
12.2、内存测试算法	316
12.2.1 0-1 算法	317
12.2.2 棋盘算法(Checkerboard algorithm).....	318
12.2.3 跳图算法(Gallop Algorithm)	319
12.2.4 步进算法(Walking Pattern Algorithm).....	320
12.2.5 平移跳跃算法(Sliding Galloping Algorithm).....	321
12.2.6 蝶形算法(Butterfly Algorithm)	322
12.2.7 移动反演算法(Moving Inversions Algorithm).....	324
12.2.8 邻域干扰算法(Surround Disturb Algorithm).....	325
12.2.9 行进算法(March Algorithm)	326
12.2.9.1 March 5n 算法	327
12.2.9.2 March 5n+ 算法	327
12.2.9.3 March Checkerboard 算法	329
12.2.9.4 MATS 算法	330
12.2.9.5 MATS+ 算法	330
12.2.9.6 MATS++ 算法	331

WX: lahmyyc638;QQ:3693817688;E-MAIL:3693817688@qq.com

12.2.9.7 March X 算法	331
12.2.9.8 March Y 算法	332
12.2.9.9 March A 算法	332
12.2.9.10 March B 算法	333
12.2.9.11 March C 算法	333
12.2.9.13 March C+ 算法	334
12.2.9.14 March SS 算法	335
12.2.9.15 March TBA 算法	336
12.2.9.16 March TB 算法	336
12.2.9.17 March-CW	336
12.2.9.18 March C-Rndom Number 算法	337
12.2.9.19 March C-Checkerboard 算法	337
12.2.9.20 SUMMARY	338
12.2.9.21 March-GS	339
12.2.9.22 March-M	339
12.2.9.23 March-U	339
12.2.9.24 March Test Summary	340
12.2.10 随机数算法(Random Number Algorithm)	340
12.2.11 移动反演-随机数算法(Moving Inversions, random pattern Algorithm)	341
12.3、MemTest86 内存测试算法的介绍	342
Test 0 [Address test, walking ones, no cache]	344
Test 1 [Address test, own address, 1 cpu]	348
Test 2 [Address test, own address]	349
Test 3 [Moving inversions, ones&zeros, Parallel]	351
Test 4 [Moving inversions, 8 bit pattern]	359
Test 5 [Moving inversions, random pattern]	360
Test 6 [Block move, 64 moves]	362
Test 7 [Moving inversions, 32 bit pattern]	375

WX: lahmyyc638;QQ:3693817688;E-MAIL:3693817688@qq.com

Test 8 [Random number sequence].....	382
Test 9 [Modulo 20, Random pattern]	388
Test 10 [Bit fade test, 2 patterns]	400
Test 11 [Random number sequence, 64-bit]	402
Test 12 [Random number sequence, 128-bit]	407
Test 13 [Hammer Test]	413
Test 14 [DMA Test].....	424
12.4、其他内存测试算法.....	425
第 13 章、UEFI 框架下，Intel PC CPU 的 IMC 的内存地址解码原理与代码实现(找出内存物理地址(e.g. 0X12345678ABC)到 DRAM 结构地址(SLOT/RANK/BG/BK/ROW/COI)的映射关系)	428
13.1 内存控制器的运行原理.....	428
13.2 Memory Interleaving (内存交织)	432
13.3 内存地址解码的 MRC 代码剖析	436
第 14 章、UEFI 框架下，故障内存晶体颗粒的定位	545
14.1、对于 DDR4.....	546
14.2、对于 DDR5.....	548
14.3、多条和多 Rank 条件下的故障内存颗粒定位.....	551
14.4 MT86_V10_CHIPDECODE.exe 解析软件	559

14.5 内存测试的软件汇总	567
14.5.1、《HCI MemTest, RunMemtestPro》	567
14.5.2、《MEMTEST64》	569
14.5.3、AIDA64 稳定性测试	571
14.5.4、《MEMTEST86》与《MEMTEST86+》	573
14.5.5、Windows Memory Diagnostic Tool(微软内存诊断工具)	576
14.5.6、《RAM STRESS TEST》	577
14.5.7、《AMT64 和 AMT128》	580
14.5.8、《DocMemory》	583
14.5.9、《RAMFIX V110516B》	584
14.5.10、《Smart RAM Detect 1.1》	585
14.5.11、《Memtest Jacky V1.6》	585
14.5.12、《GoldMemory》	586
14.5.13、《TestMem5》	587
14.5.14、《StressAppTest》	592
14.5.15、《IMX DDR Stress Tester》	604
14.5.16、《Memtester》	609
14.5.17、《System Memory Test, SMTTest》	613
14.5.18、《台湾欧阳软件》	614

14.5.19、《Ultra Memory Stress》	620
14.6 不开机 DDR 内存的故障分析方案	624
14.6.1、可以热启动和热停机的台湾欧阳软件	624
14.6.2、美国的 CST 内存测试设备	626
14.6.3、KTI ATE 设备	631
14.6.4、定制 DEBUG 功能的 BIOS	633
14.6.5、Shmoo 分析设备	634
14.6.5.1、前言	634
14.6.5.2、Shmoo 简介	635
14.6.5.3、Shmoo 的类型	640
14.6.5.4、Shmoo 测试/Shmooing	642
14.6.5.5、Shmoo 图	643
14.6.6、服务器的 BIOS 的 RMT 分析功能	644
14.6.7、ADVANTEST ATE 设备	649
第 15 章、UEFI 框架下，hPPR 的原理与实现	653
15.1 DDR4 的 PPR 修复	653
15.1.1 硬件级的封装后修复(hPPR)	654
15.1.2 软件级的封装后修复(sPPR)	661
15.1.3 UEFI 框架下，DDR4 的 PPR 的代码实现	666
15.1.4 UEFI 框架下，LPDDR4 的 PPR 的代码实现	766
15.2 DDR5 的 PPR 修复	790
15.2.1 硬件级的封装后修复(hPPR)	793

15.2.2 软件级的封装后修复(sPPR).....	797
15.2.3 UEFI 框架下, DDR5 的 PPR 的代码实现.....	802
15.2.4 UEFI 框架下, LPDDR5 的 PPR 的代码实现.....	833
第 16 章、UEFI 框架下, 其他疑难杂症问题的总结与解答.....	854
第 17 章、UEFI 框架下, CPU 温度的获取与实现.....	858
第 18 章、UEFI 框架下, SSD、U 盘等 USB DISK 的信息获取.....	863
第 19 章、UEFI 框架下, 内存条温度的获取与实现.....	872
19.1 DDR4.....	872
19.2 DDR5.....	873
19.3、DDR5 内存的 SPD HUB.....	874
19.4、LINUX 系统下的 DIMM 温度获取的代码实现.....	883
19.5 DRAM 热量和功率优化.....	890
19.6 SMBUS 读取 DIMM 温度的代码实现.....	891
第 20 章、UEFI 框架下, 内存条电压、电流、功耗的获取与实现.....	918
20.1 DDR4.....	918
20.2 DDR5.....	918
20.3、PMIC 芯片的简介.....	919
20.4、读取实时电压、电流的代码.....	937
第 21 章、UEFI 框架下, AHCI SATA HDD 的信息获取与实现.....	945

21.1、DISK INFO PROTOCOL	945
21.2、EFI_BLOCK_IO_PROTOCOL.....	954
21.3、EFI_DISK_INFO_PROTOCOL.....	959
21.4、设计一个 Shell 下面硬盘的选择菜单.....	967
第 22 章、UEFI 框架下，float 或者 double 浮点类型的调用与实现.....	978
第 23 章、UEFI 框架下，UEFI Shell 命令详解	992
第 24 章、UEFI 框架下，CPU 频率的计算与获取	999
第 25 章、UEFI 框架下，随机数的产生机制和代码实现.....	1003
第 26 章、UEFI 框架下，在自己的 EFI 程序中调用另外一个 EFI 程序的代码实现	1009
第 27 章、UEFI 框架下，EFI 程序的 CRC32 计算与代码实现.....	1034
第 28 章、UEFI GOP 框架下，截图的代码实现.....	1038
28.1 GOP 的简介	1038
28.2 UEFI 环境下，截图的代码实现.....	1044
第 29 章、UEFI GOP 框架下，在显示器上显示 BMP 图片	1061
第 30 章、UEFI 框架下，如何计算文件的 MD5.....	1096
第 31 章、UEFI 框架下，如何计算文件的 SHA-1	1101
第 32 章、UEFI 框架下，如何实现串口输出 debug 信息.....	1106
第 33 章、UEFI 框架下，如何获取 ACPI 的 DSDT Table 信息.....	1113
第 34 章、UEFI 框架下，如何获取 eMMC 的信息	1136

第 35 章、UEFI 框架下，鼠标事件的代码实现	1146
第 36 章、UEFI 框架下，非英语语言文字在显示器上的显示	1154
36.1 汉字的显示	1154
36.2 其他非英语非汉字的语言文字显示	1159
第 38 章、UEFI 框架下，如何实现 EFI 程序的 PXE 网络启动	1166
38.1、PXE 简介	1166
38.2、PXE 工作流程	1167
38.3、MemTest86 Site 程序的 PXE 启动	1168
38.4、PXE 网络启动源码分析	1172
第 39 章、UEFI 框架下，如何读写 Flash 上的文本文件	1204
第 40 章、UEFI 框架下，PCD 的配置和使用	1214
第 41 章、UEFI 框架下，UNDI 网络协议原理与代码实现	1218
41.1 UNDI 介绍	1218
41.2 SNP 查询 UNDI	1218
41.3 SNP 调用 UNDI	1227
41.4 SNP 调用 UNDI 的流程	1234
第 42 章、UEFI 框架下，SNP 网络协议原理与代码实现	1245
42.1 SNP 代码综述	1245
42.2 SimpleNetworkDriverSupported	1247

42.3 SimpleNetworkDriverStart	1251
42.4 SNP_DRIVER	1255
42.5 EFI_SIMPLE_NETWORK_MODE	1263
42.6 EFI_SIMPLE_NETWORK_PROTOCOL	1271
42.7 SNP 代码示例	1278
第 43 章、UEFI 框架下，MNP 网络协议原理与代码实现	1280
43.1 MNP 代码综述	1280
43.2 MnpDriverBindingSupported	1285
43.3 MnpDriverBindingStart	1286
43.4 MNP_DEVICE_DATA	1291
43.5 MNP_SERVICE_DATA	1297
43.6 MNP_INSTANCE_DATA	1299
43.7 EFI_MANAGED_NETWORK_CONFIG_DATA	1309
43.8 MNP_45 EFI_SERVICE_BINDING_PROTOCOL	1327
43.9 MnpStart 和 MnpStop	1333
43.10 EFI_MANAGED_NETWORK_PROTOCOL	1341
43.11 MNP 事件	1364
第 44 章、UEFI 框架下，VLAN 网络协议原理与代码实现	1376
44.1 VLAN 综述	1376

44.2 VlanConfigDriverBindingSupported	1377
44.3 VlanConfigDriverBindingStart	1378
第 45 章、UEFI 框架下，ARP 网络协议原理与代码实现.....	1380
45.1 ARP 协议说明.....	1380
45.2 ARP 代码综述.....	1384
45.2.1 ArpDriverBindingSupported.....	1385
45.2.2 ArpDriverBindingStart	1387
45.2.3 ARP_SERVICE_DATA.....	1388
45.2.4 ARP_INSTANCE_DATA.....	1393
45.2.5 EFI_ARP_CONFIG_DATA.....	1396
45.2.6 ARP_CACHE_ENTRY.....	1398
45.3 ARP 事件	1408
45.4 ARP 的使用	1410
45.5 ARP 代码示例.....	1427
第 46 章、UEFI 框架下，IP4 网络协议原理与代码实现.....	1434
46.1 IP4 协议说明	1434
46.2 IP4 头部	1437
46.3 IP 地址	1438
46.4 路由.....	1441

46.5 IP 相关的协议.....	1444
46.6 IP4 代码综述.....	1447
46.7 IP4 事件	1510
46.8 IP4 代码示例	1531
第 47 章、UEFI 框架下, UDP4 网络协议原理与代码实现.....	1543
47.1 UDP4 协议说明	1543
47.2 UDP4 代码综述.....	1544
第 48 章、UEFI 框架下, TCP4 网络协议原理与代码实现.....	1582
48.1 TCP4 协议说明	1582
48.2 TCP4 代码综述.....	1586
第 49 章、UEFI 框架下, DNS4 网络协议原理与代码实现.....	1609
49.1 DNS4 协议说明	1609
49.2 DNS4 代码综述.....	1612
第 50 章、UEFI 框架下, DHCP4 网络协议原理与代码实现	1627
50.1 DHCP4 协议说明	1627
50.2 DHCP4 代码综述.....	1632
第 51 章、UEFI 框架下, MTFTP4 网络协议原理与代码实现	1652
51.1 MTFTP4 协议简介.....	1652
51.2 MTFTP4 代码综述.....	1652

第 52 章、UEFI 框架下，汇编代码的使用与代码实现.....	1659
第 53 章、UEFI 框架下，JSON 库的使用与代码实现	1663
53.1 JSON 简介.....	1663
53.2 UEFI 下使用 JSON	1665
第 54 章、UEFI 框架下，KCS 通信协议和 IPMI 命令的代码实现.....	1673
54.1 KCS 数据	1673
54.2 KSC 通信	1677
54.3 IPMI 命令介绍.....	1686
第 55 章、UEFI 框架下，NVRAM 的读写与代码实现.....	1692
55.1 NVRAM 的简介.....	1692
55.2 NVRAM 的读取.....	1695
55.3 NvRam 空间在 BIOS Bin 文件的位置.....	1697
第 56 章、UEFI 框架下，DMA 的读写与代码实现	1701
56.1 DMA 的简介	1701
56.2 DMA 的代码示例	1702
第 57 章、UEFI 框架下，PCIe 总线的读写与代码实现.....	1702
57.1 PCI/PCIe 简介	1702
57.2 PCIe 拓扑结构	1704
57.3 UEFI 环境下访问 PCI/PCIe 设备	1708

57.4 访问 PCI/PCIe 设备的代码实现.....	1711
第 58 章、UEFI 框架下, BIOS 下的 NVMe 驱动与代码实现	1736
58.1 NVMe 的历史.....	1736
58.2 BIOS 下的 NVMe 驱动	1741
第 59 章、UEFI 框架下, Openssl 工具的使用与代码实现.....	1752
第 60 章、UEFI 框架下, CXL 内存的测试与代码实现.....	1777
60.1 背景.....	1777
60.2 CXL 的应用场景.....	1780
60.3 CXL 时间线.....	1782
60.4 CXL 协议(CXL 的 3 种模式).....	1783
60.5 CXL 协议的使用案例.....	1786
60.6 CXL 技术的特征.....	1791
60.7 CXL 技术的应用.....	1793
60.8 计算机系统中的应用	1796
60.9 数据中心中的应用	1796
60.10 人工智能领域中的应用.....	1797
60.11 CXL 技术与其他技术的对比.....	1798
60.12 结论.....	1800
60.13 UEFI 框架下, CXL 内存的测试与代码实现.....	1801

第 61 章、UEFI 框架下，Disk(HDD、SSD、USB Flash Storage、SD-Card 等等)的测试与 代码实现.....	1918
61.1 HDD(Hard Disk Drive, 机器硬盘).....	1918
61.2 SSD(Solid State Drive, 固态硬盘).....	1924
第 62 章、UEFI 框架下，HOB 的使用与代码实现.....	1998
第 63 章、UEFI 框架下，VFR/HFR 的使用与代码实现.....	2047
第 64 章、UEFI 框架下，SMM 系统管理的使用与代码实现.....	2047
第 65 章、UEFI 框架下，S3/S4/S5 深度休眠的机制与代码实现.....	2060
65.1 ACPI 系统架构流程.....	2061
65.2 ACPI 可以实现的功能包括.....	2062
65.3 ACPI 表.....	2062
65.4 ASL.....	2069
65.5 ACPI 睡眠状态之 S3.....	2071
65.6 X86 架构平台的电源管理的 SX 状态和 GX 状态.....	2073
65.6.1 SX 状态.....	2073
65.6.2 GX 状态(Global system state).....	2075
第 66 章、UEFI 框架下，SlimBootloader、FSP 的技术机制与代码实现.....	2111
66.1 FSP 介绍.....	2111
66.2 FSP 的编译.....	2114

66.3 FSP 的使用.....	2115
66.4 Windows 下的编译.....	2117
66.5 Slim Bootloader 的使用	2122
第 67 章、UEFI 框架下, FDF 文件内部的组成与代码实现.....	2124
67.1 FDF 的简介	2124
67.2 基本语法	2128
67.3 代码剖析	2133
第 68 章、UEFI 框架下, RSA 加密算法的原理与代码实现.....	2144
68.1 RSA 的基本知识和操作方式.....	2144
68.2 UEFI 下的 RSA 算法的使用	2158
第 69 章、UEFI 框架下, MailBox 核间通信原理与代码实现.....	2161
第 70 章、 UEFI 框架下, 物理地址与虚拟地址相互转换的代码实现.....	2162
第 71 章、UEFI 框架下, CPU Cache 打开与关闭的代码实现.....	2164
71.1 Cache 简介.....	2164
71.2 cache 和主存之间的三种映射	2168
71.2.1 直接映射缓存.....	2169
71.2.2 组映射缓存	2174
71.2.3 全映射缓存	2176
71.2.4 三种映射模式对比	2179

第 72 章、UEFI 框架下，多核多线程的同步与互斥中，互斥锁、自旋锁、信号量的使用与代码实现.....	2180
72.1 同步与互斥的概念.....	2180
72.2 互斥锁（同步）.....	2181
72.3 自旋锁（同步）.....	2187
72.4 信号量（同步与互斥）.....	2193
第 73 章、UEFI 框架下，PPI 接口的使用与代码实现.....	2201
73.1 概念定义.....	2201
73.2 代码实现.....	2202
第 74 章、UEFI 框架下，SSD 主控 FTL 固件算法设计与代码实现.....	2218
74.1 FTL（Flash Translation Layer）.....	2219
74.2 SSD FTL 算法（Flash Translation Layer）.....	2222
74.3 FTL 映射管理.....	2225
74.3.1 块映射.....	2225
74.3.2 页映射.....	2226
74.3.3 混合映射.....	2227
74.4 FTL 映射基本原理.....	2230
74.5 FTL 映射表刷新.....	2237
74.6 FTL 垃圾回收(Garbage Collection,GC).....	2238

74.7 FTL 磨损平衡(Wear Leveling)	2245
74.8 FTL 掉电保护(Power Loss Protection)	2246
74.9 坏块管理	2249
74.10 读干扰和数据保持(RD&DR)	2252
74.11 SSD 基本工作原理	2259
74.11.1 SSD 写数据操作	2261
74.11.2 SSD 读数据操作	2261
74.11.3 SSD 性能测试.....	2262
74.12 SSD 系统架构	2262
74.13 FTL 算法的设计思路与代码实现.....	2265
74.13.1 Address Mapping 算法.....	2271
74.13.1.1、page-level mapping	2274
74.13.1.2、block-level mapping.....	2277
74.13.1.3、hybrid-level mapping.....	2279
74.13.1.4、variable length mapping.....	2284
74.13.2 Hot/Cold Data Identification 算法.....	2291
74.13.2.1、Bloom Filter	2291
74.13.2.2、WDAC	2295
74.13.2.3、LRU	2297
74.13.2.4、Misc 方法	2302
74.13.3 GC 和 WL 的特性和算法	2304
74.13.3.1、BAGC (Buffer-Aware GC)	2308
74.13.3.2、SAGC (Swap-Aware GC)	2309
74.13.3.3、LINK-GC.....	2310
74.13.3.4、Lazy-RTGC.....	2312
74.13.3.5、Reinforcement Learning-Assisted GC	2314

74.13.4 Power off Recovery 算法	2320
74.13.4.1、Interleaving Prebackup	2324
74.13.4.2、Copyback Prebackup	2325
74.13.4.3、Parity Page Prebackup	2326
74.13.5 Cache Manager 算法	2330
74.13.5.1、WIPPA (Write Intensive Page Preserving Algorithm)	2332
74.13.5.2、CLC (Cold and Largest Cluster Policy)	2334
74.13.5.3、MaCACH	2335
74.13.5.4、RFLRU (Random First LRU)	2337
74.13.5.5、C-lash Cache System	2340
74.14 示例 1: subpage-level mapping FTL 设计概要	2342
74.15 示例 2: a generic FTLs interface and device interface for SSD on the Linux system 设计	2404
74.16 示例 3: About Implementation of SSD FTL firmware with hybrid log-block mapping, garbage collection and wear leveling	2426
74.17 示例 4: a fast & accurate simulator for modern multi-queue (MQ) and SATA SSDs	2428
74.18 示例 5: Physical Space Reallocation for 3-D Flash	2488
74.19 示例 6: a simple project to simulate SSD behavior and page mapping FTL	2583
第 75 章、UEFI 框架下，内存 EDAC 检测和 MCA 功能的代码实现	2595
75.1 EDAC 的定义	2595
75.2 LINUX 系统下 EDAC 工具的使用	2597
75.3 LINUX 系统下 EDAC 功能的源码剖析	2598

第 76 章、UEFI 框架下，INTEL XEON 服务器处理器的 RETRY_RD_ERR_LOG 机制的原理和代码实现	2644
第 77 章、UEFI 框架下，Intel PC CPU 的 IMC 的内存地址编码原理与代码实现(找出 DRAM 结构地址(SLOT/RANK/BG/BK/ROW/COL) 到内存物理地址(e.g. 0X12345678ABC)的映射关系)	2654
第 78 章、服务器基础知识和 UEFI 框架下，Intel Server CPU 的 IMC 的内存地址解码原理与代码实现(找出内存物理地址(e.g. 0X12345678ABC)到 DRAM 结构地址(SLOT/RANK/BG/BK/ROW/COL)的映射关系)	2740
78.1 服务器的基础知识	2740
78.2 代码剖析	2774
第 79 章、UEFI 框架下，Intel Server CPU 的 IMC 的内存地址编码原理与代码实现(找出 DRAM 结构地址(SLOT/RANK/BG/BK/ROW/COL) 到内存物理地址(e.g. 0X12345678ABC)的映射关系)	2836
第 80 章、UEFI 框架下，AMD PC CPU 的 UMC 的内存地址解码原理与代码实现(找出内存物理地址(e.g. 0X12345678ABC)到 DRAM 结构地址(SLOT/RANK/BG/BK/ROW/COL)的映射关系)	2891
第 81 章、UEFI 框架下，AMD PC CPU 的 UMC 的内存地址编码原理与代码实现(找出 DRAM 结构地址(SLOT/RANK/BG/BK/ROW/COL) 到内存物理地址(e.g. 0X12345678ABC)的映射关系)	2915

第 82 章、UEFI 框架下，AMD Server CPU 的 UMC 的内存地址解码原理与代码实现(找出内存物理地址(e.g. 0X12345678ABC)到 DRAM 结构地址

(SLOT/RANK/BG/BK/ROW/COL)的映射关系) 2931

第 83 章、UEFI 框架下，AMD Server CPU 的 UMC 的内存地址编码原理与代码实现(找出 DRAM 结构地址(SLOT/RANK/BG/BK/ROW/COL) 到内存物理地址(e.g.

0X12345678ABC)的映射关系) 2981

第 84 章、UEFI 框架下，ARM64 PC CPU 的 DMC 的内存地址解码原理与代码实现(找出内存物理地址(e.g. 0X12345678ABC)到 DRAM 结构地址

(SLOT/RANK/BG/BK/ROW/COL)的映射关系) 2991

第 85 章、UEFI 框架下，ARM64 PC CPU 的 DMC 的内存地址编码原理与代码实现(找出 DRAM 结构地址(SLOT/RANK/BG/BK/ROW/COL) 到内存物理地址(e.g.

0X12345678ABC)的映射关系) 3014

85.1 Bootloader 的介绍 3014

85.2 Bootloader 的启动 3015

85.3 Bootloader 的种类 3016

85.4 U-Boot 介绍 3019

85.5 U-Boot 源码结构 3020

第 86 章、UEFI 框架下，ARM64 Server CPU 的 DMC 的内存地址解码原理与代码实现(找出内存物理地址(e.g. 0X12345678ABC)到 DRAM 结构地址

(SLOT/RANK/BG/BK/ROW/COL)的映射关系) 3061

第 87 章、UEFI 框架下, ARM64 Server CPU 的 DMC 的内存地址编码原理与代码实现 (找出 DRAM 结构地址(SLOT/RANK/BG/BK/ROW/COL) 到内存物理地址(e.g. 0X12345678ABC)的映射关系).....	3068
第 88 章、UEFI 框架下, OptionRom 的固件驱动与代码实现.....	3069
第 89 章、UEFI 框架下, UEFI BIOS ROM 文件的编译流程与详细说明.....	3143
89.1 UEFI BIOS 的 Build 流程.....	3143
89.2 搭建 UEFI BIOS 编译的步骤.....	3155
89.3 uefi-tools 编译 edk2 实践.....	3158
89.4 UEFI 工程文件之间的关联.....	3166
89.5 EDK II 模块.....	3189
89.6 EDK II 实现 UEFI Application.....	3191
89.7 EDK II 实现 UEFI Driver.....	3193
89.8 UEFI Build 实践.....	3195
第 90 章、UEFI 框架下, JPEG 格式图片显示的代码实现.....	3238
第 91 章、UEFI 框架下, DDR4 的 SPD 数据解读.....	3263
第 92 章、UEFI 框架下, DDR5 的 SPD 数据解读.....	3270
第 93 章、UEFI 框架下, LPDDR4/4X 的 SPD 数据解读.....	3279
第 94 章、UEFI 框架下, LPDDR5/5X 的 SPD 数据解读.....	3280
第 95 章、UEFI 框架下, DDR4 JESD 的注释解读.....	3280

95.1 DDR4 SDRAM 的引脚封装与寻址	3281
95.2 DDR4 状态转换图	3287
95.3 寄存器定义	3294
95.4 DDR4 SDRAM 命令描述与操作	3307
95.5 tRFC 与 tREFI 参数	3330
95.6 多功能寄存器 (MPR)	3334
95.7 数据掩码 (DM) , 数据总线翻转 (DBI) , 以及 TDQS	3349
95.8 DRAM 单片可寻址能力	3362
95.9 CRC	3370
95.10 命令、地址总线奇偶校验 (C/A Parity)	3384
95.11 控制器降档模式 (Controller Gear Down Mode)	3394
95.12 DDR4 核心时序	3398
95.13 可编程的先导区域	3400
95.14 读操作	3405
95.15 写操作	3432
第 96 章、UEFI 框架下, DDR5 JESD 的注释解读	3490
第 97 章、UEFI 框架下, LPDDR4/4X JESD 的注释解读	3628
第 98 章、UEFI 框架下, LPDDR5/5X JESD 的注释解读	3655
第 99 章、UEFI EDKII 框架下, DDR4 Memory Training Flow 与源码分析	3789

99.1 基本流程	3789
99.2 DDR4 基他训练	3799
第 100 章、UEFI EDKII 框架下，DDR5 Memory Training Flow 与源码分析	3803
100.1 基本流程	3803
100.2 DDR 为什么要进行 Training 训练?	3806
100.3 Read Training.....	3806
100.3.1 Read Training 的操作	3808
100.3.2 MR26-MR30 寄存器	3809
100.3.3 通过 MR26-27 寄存器设置	3816
100.3.4 Read Training Pattern Examples	3818
100.3.5 Read Training Pattern Timing Diagrams	3822
100.3.6 Read Preamble Training Mode	3824
100.3.7 LoopBack 在 DDR5 的应用	3827
100.4 CA Training Introduction.....	3840
100.5 CS Training MODE	3844
100.6 DDR5 的 Writing training.....	3848
100.6.1 Introduction	3849
100.6.2 MCU 如何对于 Write Level 进行调整的?	3850
100.6.3 Write Leveling Mode Registers	3853

100.6.4 External Write Leveling Training Operation	3855
100.6.5 DRAM Termination During Write Leveling	3863
100.6.6 Write Pattern Command	3863
100.7 DDR5 支持的 CT 模式	3866
100.8 Pin Mapping.....	3867
100.9 Logic Equations	3868
100.10 代码示例	3869
100.11 DDR4 与 DDR5 训练流程的差异	3874
第 101 章、UEFI 框架下，VeraCrypt 的使用和源代码分析	3875
第 102 章、UEFI 框架下，BIOS 启动的详细介绍与代码分析	3886
102.1 BIOS 启动流程简介	3886
102.2 阶段一：SEC (Security Phase) 安全验证阶段	3887
102.2.1 SEC 阶段的功能	3888
102.2.2 SEC 阶段的执行流程	3888
102.3 阶段二：PEI (Pre-EFI Initialization) 前期初始化阶段	3896
102.3.1 PEI 阶段的执行流程	3896
102.3.2 具体调用的系统中的 PEIM 如下	3901
102.3.3 PEI 阶段的功能	3901
102.3.4 PEI 划分	3902

102.3.5 为什么要有 PEI Phase	3903
102.3.6 PEI 代码流程分析	3903
102.3.7 PEI Core 分析	3909
102.3.7.1 PEI Foundation	3910
102.3.7.2 PEIM	3911
102.3.7.3 PEI Dispatcher	3915
102.3.7.4 PeiServices	3919
102.4 阶段三: DXE (Driver Execution Environment) 驱动执行环境阶段	3965
102.4.1 DXE 阶段的执行流程	3966
102.4.2 DXE 阶段的功能	3968
102.4.3 涉及到的元件及功能	3968
102.4.4 DXE Architecture Protocol 种类及其功能	3969
102.5 阶段四: BDS (Boot Device Select) 启动设备选择阶段	3969
102.5.1 BSD 阶段执行流程	3972
102.5.2 BDS Steps	3975
102.5.3 执行策略	3976
102.5.4 BDS 三大任务	3977
102.6 阶段五: TSL(Transient System Load)操作系统加载前期阶段	3977
102.7 阶段六: RT(Run Time)运行阶段	3979
102.8 阶段七: AL(After Life)灾难恢复阶段	3979
第 103 章、半导体芯片失效分析(Failure Analysis)	3980

第 104 章、DRAM 失效案例分析(Failure Analysis).....	4053
104.1 引子	4053
104.2 内存的演化历史	4055
104.3 半导体存储器的分类	4060
104.4 DRAM 技术的演化历史	4071
104.5 LPDDR 技术的演化历史	4082
104.6 DRAM 基本工作原理	4087
104.7 DRAM 总体设计	4119
104.7 常用操作的时序	4126
104.8 ODT 片内端接电阻	4150
104.9 ZQ 校准	4153
104.10 DRAM 制造工艺	4160
104.11 DRAM 芯片选型示例	4184
104.12 内存测试方案和流程	4189
104.13 不良内存的实例分析	4196
第 105 章、FLASH 失效案例分析(Failure Analysis)	4215

电子书更新说明

版本号	更新日期	更新说明
V0.1	20220816	1、本电子书诞生了，这是它的第一个版本； 2、内容还不充实，目录也不能跳转。
V0.2	20230408	1、新增了很多新章节，扩大了电子书覆盖面； 2、对部分章节内容进行了调整和充实。
V0.3	20231128	1、新增了很多新章节，扩大了电子书覆盖面； 2、对部分章节内容进行了调整和充实； 3、在电子书里面增加大量的源代码引用和说明，增加读者对知识的深度了解。
V0.4	20240609	1、继续新增了很多新章节，扩大了电子书覆盖面； 2、对部分章节内容进行了调整和充实； 3、对一些不合理的排版进行了重新调整和布局； 3、继续在电子书里面增加大量的源代码引用和说明，增加读者对知识的深度了解。
V0.5	20250211	1、新增了一些章节内容，使得电子书涵盖的内容更加广泛； 2、充实了部分章节的内容； 3、新增了 INTEL 和 AMD 服务器的内存控制器的讲解章节，并附带了源代码剖析。
V0.6	20250411	1、继续新增了一些章节内容，使得电子书涵盖的内容更加广泛； 2、继续充实了部分章节的内容； 3、新增了 ARM64 平台的 DMC 内存控制器的解析和源代码剖析； 4、为了迎合不同读者的需求，将电子书分别为 A、B、C、D 四个不同版本，价格依次递增。
V0.7	20250711	1、目录终于可以跳转了，方便读者快速跳转到目标页数； 2、继续充实了部分章节的内容； 3、新增了一些章节内容，使得电子书涵盖的内容更加广泛。
V0.8	20250814	1、将 3 级目录升级为 4 级目录，方便读者更加清晰的对每章的内容有所了解； 2、增加了页码，方便读者用手机阅读时，清楚的记得自己所在的页码位置，方便下次继续阅读； 3、增加了第 0 章，这一章内容是为了方便小白读者，介绍如何一步步的搭建基于 EDKII 的 UEFI APP 开发编译环境； 4、在第 0 章中，增加了 UEFI BIOS 的开发编译环境以及调

WX: lahmyyc638;QQ:3693817688;E-MAIL:3693817688@qq.com

		试方法，对于常见的 AMI、Insyde、百教的 BIOS 开发环境搭建，分别进行了讲解说明； 5、增加了 QQ 和邮箱的联系方式，电子书水印也同步了。
--	--	---

WX: lahmyyc638;QQ:3693817688;E-MAIL:3693817688@qq.com

WX: lahmyyc638;QQ:3693817688;E-MAIL:3693817688@qq.com

序言

如何获得该 PDF 电子书?

添加本人微信账号(lahmyyc638), 成交付款(微信、支付宝或者闲鱼)成功后, 亲自发送《UEFI BIOS&APP 编程开发查询手册》PDF 电子书给您。

购买成功后, 您将获取如下的权限:

- 1、此书会不定时更新, 购买过的同学可以在半年内免费获得此书的最新版本;
- 2、一年内, 可以就此书的内容进行免费咨询, 书本外的内容也欢迎交流;
- 3、本书内容所涉及的源代码分为开源代码和非开源代码, 开源代码的下载地址在书中都已经给出, 而非开源的需要额外签订保密协议和收费。

温馨提示

由于本书是 PDF 电子书, 不同于传统的纸质实体书籍, 本电子书一旦发售给用户, 不可退款, 敬请谅解, 谢谢理解! 同时本人非常欢迎已经购买的用户和本人达成合作, 经由合作伙伴推荐的购书者如果成功购买, 可以获取获得

此次交易额的一定比例的分成奖励!

警告

未经本人同意, 严禁转发或者售卖! 一经发现, 该协议服务作废, 概不退款, 同时追缴非法获利所得! 而且本人保留起诉和追究的权利!



为什么要整理成书?

市面上, 网络上, 关于 UEFI BIOS&APP 编程开发的信息形形色色、零零总总, 系统成册的却屈指可数, 例如:

《UEFI 编程实践 (罗冰)》、《UEFI 与 EDKII 源代码分析》、《UEFI 原理与编程_戴正华(著) 机械工业出版社_完整版》、《UEFI 内核导读》。

如果想深度学习了解 UEFI BIOS 的工作流程和原理，目前只有百教软件的视频培训课程：

<https://cloudclass.zqkong.com/hall>

课程专题

- 吴平: 知乎大神“老黑”，带你一起学BIOS
- 飞腾S5000C CRB介绍
- FSP技术
- ByoCore 2.0

基础培训篇

- RISC-V介绍、启动流程和应用
- BMC IPMI 概述
- BIOS从入门到精通
- UEFI & EDK II Training

中级培训篇

- FSP技术
- TPM2.0 和 度量启动
- ACPI 讲解
- SEL介绍

























高级培训篇

- 虚拟媒体与 USB gadget 相关
- OPEN-BMC
- Redfish开发介绍
- BMC & BIOS升级原理介绍

但是，这高昂的价格，不是我们个人可以承受的。

基于目前的行业现状，结合自己存储行业十余载的经验，觉得应该自己书写、归纳、总结一套 UEFI 开发工程师必备的随时可以查阅，用于编程开发的手册书籍，于是《UEFI BIOS&APP 编程开发查血手册》应运而生。

此外其他额外的电子书资料参考如下：

-  [Beyond BIOS][Developing with the Unified Extensible Firmware Interface][...
-  《UEFI内核导读》
-  《UEFI内核导读》-样章20210318
-  ACPI_6_3_May16
-  Beyond_BIOS_Second_Edition_Digital_Edition_(15-12-10)破解_index
-  Beyond_BIOS_中文预览版V0.2
-  Driver Writer's Guide
-  EDK2 UEFI BIOS windows编译方法
-  EDKII UEFI APP编译环境搭建说明文档
-  edk-ii-dec-specification
-  edk-ii-dsc-specification
-  PCI_Express_Base_r3.0_10Nov10
-  PI_Spec_1_7_A_final_May1
-  SMBIOS_DSP0134_3.4.0a
-  UEFI Spec 2.8B May 2020
-  UEFI_Shell_2_2
-  UEFI编程实践 (罗冰)
-  UEFI与EDKII源代码分析
-  UEFI原理与编程
-  UEFI原理与编程_戴正华(著) 机械工业出版社_完整版
-  从零开始的UEFI裸机编程
-  飞腾CPU UEFI BIOS固件生成教程 2022年
-  利用 UEFI 实现 内存测试，仅为方法总结，程序未提供
-  一个UEFI引导程序的实现 (田宇)

有需要的同学，可以找我额外购买获取。

另外，本书里面涉及大量的 DRAM 内存和 FLASH 存储有关的内容和代码剖析，在阅读代码之前可以先打好