ICS 35.080
L 40

中华人民共和国国家标准

GB/T 29827—2013

信息安全技术　可信计算规范
可信平台主板功能接口

Information security technology—Trusted computing specification—Motherboard function and interface of trusted platform

2013-11-12 发布　　2014-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

GB/T 29827—2013

中华人民共和国
国家标准
信息安全技术　可信计算规范
可信平台主板功能接口
GB/T 29827—2013
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323　发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 2.75　字数 80 千字
2014年3月第一版　2014年3月第一次印刷
*
书号:155066·1-48051　定价 39.00 元

GB/T 29827-2013

目　　次


```
typedef UEFI_STATUS (UEFIAPI * TPCM_SCH_EXTEND) (
IN UINT8 * InDigest,
IN UINT32 pcrNum
);
```

参数说明见表 49。

表 49　TPCM_SCH_EXTEND 函数参数描述

数据	描述
InDigest	指向杂凑结果的指针
pcrNum	将要扩展杂凑结果的 PCR

TPCM_SCHExtend()可以将 32 字节长的杂凑结果扩展到特定的 PCR 中，该方法是唯一改变 PCR 内容的方法。该函数能够将软件 SCH 计算出的杂凑结果扩展到 PCR 中从而减轻 TPCM 的运算工作量。

返回的状态代码见表 34。

11.3.2.17　UEFI_TPCM_OP_PROTOCOL.TPCM_ SCH_SelfTest ()

TPCM_SCH_SelfTest()用于检测 HW 的 SCH 是否能正常工作。其原型如下：

```
typedef UEFI_STATUS (UEFIAPI * TPCM_SCH_SELF_TEST) (
IN UINT8 * HashData,
IN UINT32 HashDataLen,
IN UINT32 PcrNum
);
```

参数说明见表 50。

表 50　TPCM_SCH_SELF_TEST 函数参数描述

数据	描述
HashData	输入参数，为指向待 Update 数据的指针
UpdateDataLen	输入参数，描述 HashData 的长度
PcrNum	杂凑结果将要扩展到的 PCR

TPCM_SCH_SelfTest()为 SCH 硬件引擎测试程序，该函数中调用了 TPCM_SCHStart()、TPCM _ SCHUpdate ()、TPCM_SCHCompleteExtend ()等。

返回的状态代码见表 51。

表 51　TPCM_SCH_SelfTest()状态返回码

UEFI_SUCCESS	SCH 测试通过
UEFI_DEVICE_ERROR	芯片无响应，查看是否发送参数错误

11.3.2.14 UEFI_TPCM_OP_PROTOCOL.TPCM_SCHUpdate ()

TPCM_ SCHUpdate ()将传入的数据做 Update 的操作，每次 Update 的长度最大长度为 64 字节。其原型如下：

```
typedef UEFI_STATUS (UEFIAPI * TPCM_SCH_UPDATE) (
IN UINT8 * HashData,
IN UINT32 UpdateDataLen
);
```

参数说明见表 47。

表 47 TPCM_SCH_UPDATE 函数参数描述

数据	描述
HashData	输入参数，为指向待 Update 数据的指针
UpdateDataLen	输入参数，描述 HashData 的长度

使用 TPCM_SCHUpdate ()在效率上将明显的低于使用软件 SCH 实现，推荐使用本规范中 SCH 的软件算法实现，但从安全性角度考虑，仍支持硬件实现。

UpdateDataLen 不能大于 64 字节，否则大于 64 字节部分内容不能正确的 Update 到 TPCM 芯片的 SCH 算法引擎，若需要 Update 的数据量较大时，可以通过多次调用 TPCM_SCHUpdate()来实现。

返回的状态代码见表 34。

11.3.2.15 UEFI_TPCM_OP_PROTOCOL.TPCM_SCHCompleteExtend ()

TPCM_SCHCompleteExtend ()将传入的数据以及 Update 的内容扩展到对应的 PCR 寄存器中，每次 CompleteExtend 的长度最大长度为 64 字节。其原型如下：

```
typedef UEFI_STATUS (UEFIAPI * TPCM_SCH_COMPLETE_EXTEND) (
IN UINT8 * HashData,
IN UINT32 UpdateDataLen,
IN UINT32 PcrNum
);
```

参数说明见表 48。

表 48 TPCM_SCH_COMPLETE_EXTEND 函数参数描述

数据	描述
HashData	输入参数，为指向待 Update 数据的指针
UpdateDataLen	输入参数，描述 HashData 的长度
PcrNum	Complete 的结果将要扩展到的 PCR

SCHCompleteExtend 不能大于 64 字节，否则大于 64 字节部分内容不能正确的 Update 到 TPCM 芯片的 SCH 算法引擎，若需要处理的数据量较大时，可以通过多次调用 TPCM_SCHUpdate()最后在调用 TPCM_SCHCompleteExtend 来实现。

返回的状态代码见表 34。

11.3.2.16 UEFI_TPCM_OP_PROTOCOL.TPCM_ SCHExtend ()

TPCM_SCHExtend()将杂凑结果扩展到对应的 PCR 寄存器。其原型如下：

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准主要起草单位：北京工业大学、中国长城计算机深圳股份有限公司、南京百敖软件股份有限公司、航天科工集团二院七〇六所、武汉大学、中国电子科技集团公司信息化工程总体研究中心、北京龙芯中科技术服务中心有限公司、江南计算技术研究所、瑞达信息安全产业股份有限公司、中安科技集团有限公司、中船重工集团 707 所、北京中科院软件研究中心、北京华大恒泰科技有限责任公司、北京超毅世纪网络技术股份有限公司、华为技术有限公司、桂林长海科技有限责任公司、中国电子技术标准化研究所。

本标准主要起草人：沈昌祥、韩永飞、张兴、王冠、林诗达、徐明迪、王正鹏、蒋志翔、赵丽娜、周艺华、石明、张斌、孔雷、张焕国、汪文杰、胡明昌、吴新军、陈林、李大东、王然、张向阳、艾方、童广胜、徐庶桓、李晨、贾兵、杜中平、杜晖、谢乾、赵波、张超、吴勇、石良军、马银生、郭景川、魏靖、宋洋、高瞻、曲新春、余发江、陈小春、蔡晔、袁爱东、庄琭、曾颖明、孙永泉、段丽娟、宋靖、朱贺新、郭灵儿、刘智君、滕志刚、靳淳、郭毅、肖祎、孙圣超、刘军，陈莹，邹娜。