软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(Suppl.(2)):229−235

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于信号完整性分析的 TPM 芯片设计*

陈 曦[1,2]

[1](招商银行总行 博士后科研工作站,广东 深圳 518067)

[2](招商银行总行 信息技术部,广东 深圳 518057)

通讯作者: 陈曦, E-mail: cx8408@hotmail.com, http://www.cmbchina.com

摘 要: 由于可信计算平台自身的设计原理及机制上的缺陷,其在面对物理攻击时很难有效地保护整个平台系统的安全性,而基于信号完整性分析的 TPM 芯片设计思想已给出了较好的解决方案.在上述研究工作的基础上,进一步提出了逻辑分层的 TPM-APM(TPM-analog parameter measurement)子模块改进设计方案.通过对时延模拟参数的度量,给出了 TPM 芯片中 TPM-APM 子模块的工程实现方法,并使用眼图比对法,为 TPM-APM 子模块实现的可行性进行了验证.分析结果表明,引入改进设计的 TPM-APM 子模块可增强可信计算平台面对物理攻击时的防御能力.

关键词: 可信计算;物理攻击;TPM;信号完整性分析;时延

中文引用格式: 陈曦.基于信号完整性分析的 TPM 芯片设计.软件学报,2013,24(Suppl.(2)):229−235. http://www.jos.org.cn/1000-9825/13041.htm

英文引用格式: Chen X. Design of TPM chip based on signal integrity analysis. Ruan Jian Xue Bao/Journal of Software, 2013, 24(Suppl.(2)):229−235 (in Chinese). http://www.jos.org.cn/1000-9825/13041.htm

Design of TPM Chip Based on Signal Integrity Analysis

CHEN Xi[1,2]

[1](Department of Post-Doctoral Research Center, China Merchants Bank, Shenzhen 518067, China)

[2](Department of Information Technology, China Merchants Bank, Shenzhen 518057, China)

Corresponding author: CHEN Xi, E-mail: cx8408@hotmail.com, http://www.cmbchina.com

Abstract: Due to the defects caused by design principle and mechanism, Trusted Computing Platform can't effectively protect the system security from physical attacks. A novel design method based on signal integrity analysis was introduced to solve this problem. Based on the work stated above, this paper proposes a revised logical hierarchical design of TPM-APM (TPM-analog parameter measurement) sub-module. Furthermore, engineering implementation method of TPM-APM sub-module is provided by measuring the analog parameters of delay. Through comparing eye patterns, the practicability of implementing the TPM-APM sub-module is verified. Detailed analysis and experiment reveal that the revised TPM-APM sub-module can effectively enhance the ability of protecting Trusted Computing Platform against physical attacks.

Key words: trusted computing; physical attack; TPM; signal integrity analysis; delay

随着全球信息化的不断深入,我们的生活越来越依赖于计算机与 Internet.然而计算机系统与网络的开放性与互联性在方便我们生活的同时,也带来了众多始料未及的安全问题.传统的信息安全系统主要通过防火墙、入侵检测、防病毒软件等被动防御安全体系进行构建[1],其面对日益繁杂的攻击,已很难有效地保障信息的安全.另一方面,现有的网络应用模式将服务器与网络作为安全防御重点,却忽略了对接入网络终端计算机的安全防范,这样的设计缺陷也进一步加剧了计算机系统的脆弱性与危险性.如果能够从计算机网络终端进行主动防御,从各个源头控制整个信息系统的安全,将有效地解决目前众多难于控制的安全问题.TCG(trusted computing

* 基金项目: 国家自然基金委员会-广东联合基金(U1135002); 国家科技部重大专项(2011ZX03005-002)
收稿时间: 2013-07-17; 定稿时间: 2013-10-16

group)对可信计算概念的提出正是以此为出发点,在计算机硬件平台内部引入安全芯片 TPM(trusted platform module)[2−4],希望通过增强终端计算平台架构的安全性,进而增强整个信息系统的安全性.

TPM 芯片是可信计算平台的核心部件.它由 CPU、存储器、I/O、随机数产生器等部件组成,完成可信度量的存储、密钥产生、加密、签名等功能.TPM 是整个可信计算平台的信任根[5,6],为各种安全服务提供保护.然而,由于可信平台自身设计的原理及机制上的缺陷,可信平台在面对日益更新的物理攻击时[7−9],其硬件级保护显得十分脆弱.针对此问题,国内外研究人员做了相当多的改进工作[10,11].文献[12]中也提出了一种基于信号完整性分析的抗物理攻击 TPM 芯片设计.本文正是在文献[12]的基础上进一步提出了逻辑分层的 TPM-APM(TPM-analog parameter measurement)子模块改进设计方案,并在充分验证时延模拟参数可测性的基础上,使用 Acam 公司的高精度时间间隔测量芯片 TDC-GP1 芯片,给出了 TPM 芯片中 TPM-APM 子模块的工程实现方法.最终通过比对增加测量引线后嵌入式系统高速 SDRAM 的眼图,对 TPM-APM 子模块实现的可行性进行了验证.分析结果表明,TPM-APM 子模块的引入可增强可信计算硬件平台面对物理攻击的防御能力.

1 安全问题

TPM 芯片是可信架构最为关键的部分,用来执行整个平台完整性和可信性的检测,并为系统提供密钥产生、加密、签名等功能.但 TCG 在设计 TPM 芯片架构时,并未周全地考虑平台本身可能遭受的潜在物理攻击威胁.而随着可信计算的应用逐渐广泛,针对可信计算平台的物理攻击也接踵而至.

可信计算平台目前面临的物理攻击很大一部分属于边信道攻击(side channel attack).所谓边信道攻击,是指通过分析攻击目标的基本电路运行过程中的计算时间、功率消耗、程序运行故障、电磁辐射等泄露信息,获得平台芯片内部运算情况,从而破坏整个安全系统的攻击方法.较为流行的边信道攻击方法包括功耗攻击、计时攻击和电磁攻击等.这些攻击方法避开了信息安全系统复杂的密码算法及安全架构本身,比传统的攻击方法更加快速、有效[13].根据边信道建立途径的不同,它们可以分为被动攻击和主动攻击两类.被动攻击是在不改变密码算法的正常运算流程的前提下,通过旁路被动探测的方式分析敏感数据,如系统功耗、算法执行延迟时间等.主动攻击是通过在关键的密码模块和交互协议执行中引入差错,从而引起系统机密数据的泄露,如将攻击目标置于极端的工作环境(极高或极低的电压等)[14].此外,文献[12]中设计了一个简单、有效的攻击,通过 FPGA 的双口 RAM,在欺骗过系统的完整性度量的情况下,对可信平台进行了经典的 TOCTOU(time-to-use,time- to-check)攻击[15];在文献[16]中,Sparks 详细分析了针对 TPM 的 Reset attack 和 Timing attack;在 Black Hat 会议中,信息安全研究员 Christopher Tarnovsky 更是通过物理攻击破解了 Infineon 公司生产的 SLE 66 微控制器(该硬件基于 TCG 公布的 TPM 规范进行设计生产).种种迹象表明,随着可信计算平台的深入发展,改进 TPM 芯片设计架构以解决日益涌现的物理攻击问题迫在眉睫.

2 TPM-APM 的分层设计及工程实现

2.1 前期工作

文献[12]中提出了一种可抗物理攻击 TPM 芯片设计方法:如图 1 所示,在 TPM 芯片中增加模拟参数度量子模块 TPM-APM(TPM-analog parameter measurement),TPM-APM 使用信号完整性[17]的分析方法,通过对印制电路板的模拟参数的分析来构建一组度量函数.每次可信平台加电启动时,通过对模拟量标识进行比对来防止针对可信平台的物理攻击.

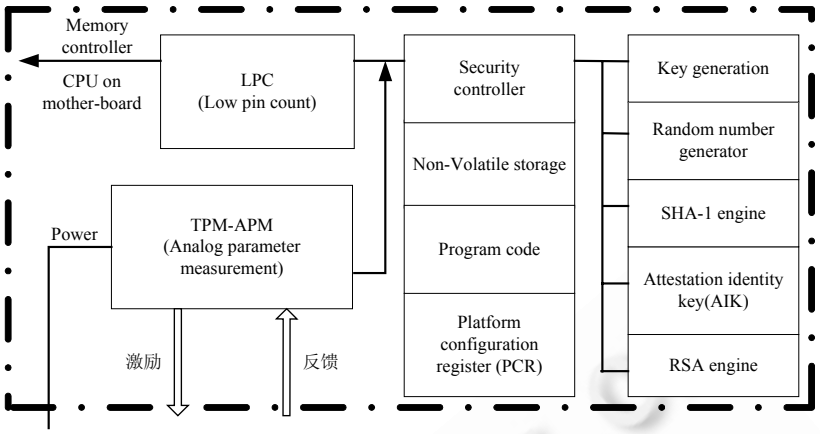


Fig.1 Architecture of TPM chip against physical attacks[12]

图 1 抗物理攻击的 TPM 芯片架构[12]

2.2 TPM-APM的分层设计

在上述研究工作的基础上,本文根据 TPM-APM 子模块的工作原理将其进一步划分为 3 层逻辑架构:网络抽象层、模拟量测量层、数据收集对比层.如图 2 所示,网络层根据印制电路板的特性对无源网络进行抽象划分、选出 n 个具有代表性的特定网络,以便能够对可信平台进行全面、高效的度量.模拟量测量层集成了时延特性测量模块、功耗特性测量模块、阻抗特性测量模块等,不同的测量模块协同工作,对平台各个特性进行系统测量.数据收集对比层则完成最后的数据处理功能,对收集到的 n 个特定网络的多个模拟特性参数进行收集处理.因为模拟量的测量总存在一定程度的细微误差,所以数据收集对比层还需对各个模拟量设计合理的门限,从而对采集到的数据通过门限进行对比、判别,并最终将判别结果交给平台安全策略管理模块处理.平台安全策略管理模块则根据收集到的多个判别结果对可信平台的安全可靠性进行评估,判断可信平台是否存在潜在的物理攻击危险,并对评估判断结果做出响应和处理.

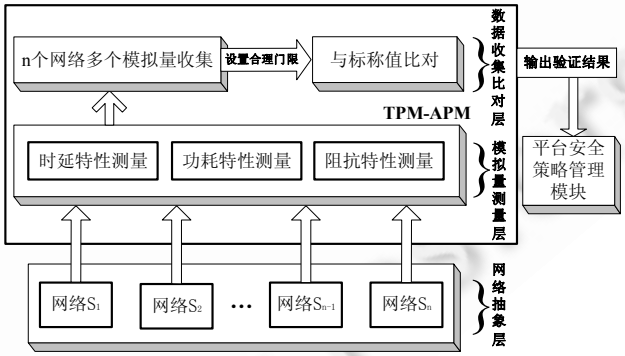


Fig.2 Hierarchical logical structure of TPM-APM

图 2 TPM-APM 分层逻辑结构图

2.3 TPM-APM的实现

下面通过时延参数的测量来说明 TPM-APM 模块在工程应用时的一种简单、可行的实现方法.对于无源网络中阻抗特性、功耗特性等模拟参数的测量,在工程上有同样成熟的理论与技术,在此不再详述.

(1) 时延参数的唯一性

时延参数反映了被测网络对激励响应的快慢,在很多系统中都是非常重要的参数,也是在考虑时序时重要

的条件.如果在可信平台安全主板的印制电路板中增加、删减或者篡改硬件,会使得特定的网络结构发生改变,而线长的变化以及走线引起的寄生电容、寄生电感的变化会导致走线的特征阻抗产生改变,进而导致时延参数的改变[18].

(2) 时延参数的可测性

系统的响应时延和信号在传输线上传播速度密切相关.信号在传输线上的传播速度从物理角度上解释,与导线周围的材料、信号在传输线导体周围空间形成的交变电磁场的建立速度和传播速度密切相关.电场和磁场建立的快慢决定了信号的速度,电磁场的传播和相互作用可以由 Maxwell 方程描述.电磁场的变化速度 v 由式(1)得到:

$$v=\frac{1}{\sqrt{\varepsilon_0\varepsilon_r\mu_0\mu_r}}\text{m/s} \tag{1}$$

其中, ε_0 表示自由空间的介电常数,值为 8.89×10^{-12}F/m; μ_0 表示自由空间的导磁率,值为 $4\pi\times10^{-7}$H/m; μ_r 表示材料的相对导磁率,值约为 1; ε_r 表示材料的相对介电常数[16].

根据时延 TD 与互联线长度的关系,可推出:

$$TD=\frac{length}{v}=length\sqrt{\varepsilon_0\varepsilon_r\mu_0\mu_r}=\frac{length\sqrt{\varepsilon_r}}{2.99792\times10^8}s \tag{2}$$

假设走线总长为 0.3m, 制板材料使用 FR4 玻纤板,其介电常数 ε_r 在 4.0~4.5 之间变化.则可估算出信号的传输时间为 2×10^{-9}s ~ 2.12×10^{-9}s, 即时延为 ns 级.而对于 ns 级的时间间隔测量,有典型的高精度测量方法——TDC(time-to-digital converter)方法[19].

(3) TDC-GP1 芯片的工程实现

对于 TPM-APM 子模块的时延参数测量,可使用 Acam 公司的高精度时间间隔测量芯片 TDC-GP1 芯片.TDC-GP1 芯片[20]拥有两个测量通道 250 ps 测量精度模式,单通道 125 ps 精度的高精度模式;每通道可最多 4 次采样,双脉冲分辨率大约为 15 ns,可再次触发;双通道的 8 个事件可多次、任意测量,无最小时间间隔限制.TPM-APM 子模块在对时延参数进行测量时,首先使用 TDC-GP1 芯片产生高速的窄脉冲并捕捉返回的脉冲,两组信号相遇后由高精度的时间间隔测量模块测量整个信号的传播时间[21].以测量数据总线的最低位为例,TPM-APM 模块与近端的 CPU 的低位数据总线相连,并且与印制板的远端控制器中的低位数据总线相连,以系统中数据总线的最低位长度的度量值作为印制板的抽象.数据总线遍布整个印制板,且大多数芯片都要与数据总线相连.因此,增加、减少或者篡改芯片,亦或是对整个系统重新布线,都会在很大程度上影响系统的时延特性.

由于 TDC-GP1 具有高精确性、高灵活性、成熟的开发环境,从而可以便捷地用它来实现 TPM-APM 模块中对时延特性的测量功能,并通过时延特性的测量完成对整个系统的硬件完整性的度量.

2.4 改进平台的工作模式

由于 TPM-APM 子模块的加入,需对现有的可信计算机的工作模式进行一定的改进.图 3 详细说明了加入 TPM-APM 子模块后的 TPM 芯片是如何配合安全 BIOS、操作系统来工作:改进的可信计算平台启动可分为 3 个部分:模拟参数度量、数字参数度量、操作系统/应用程序度量.3 个部分在图中用不同的颜色加以标识.如图 3 所示,当可信平台运行时,首先运行模拟参数度量部分,即先对 TPM-APM 子模块进行加电,TPM-APM 子模块对系统的无源网络进行模拟参数测量,并将测量值与存储的标称值进行对比.若验证失败,则发出警告,并对系统直接进行掉电处理.若验证成功,则对可信硬件平台的安全主板进行加电.随后可信硬件平台遵循传统的 TPM 安全验证模式工作:TPM 芯片与系统的安全 BIOS 配合工作,通过信任传递关系建立起可靠的信任链,逐步将硬件的可信延伸到操作系统应用级的可信.

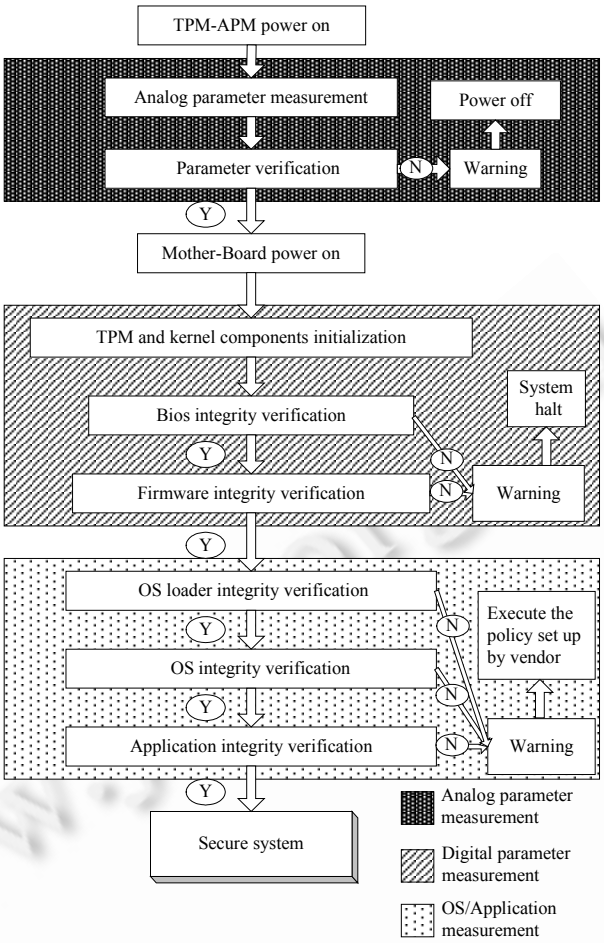


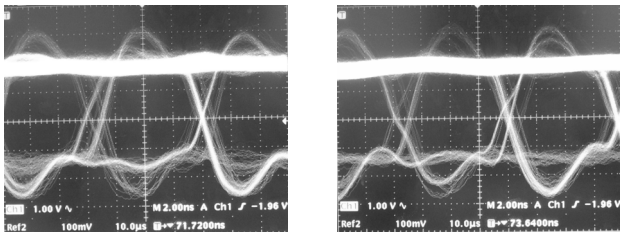
Fig.3 Trust chain transfer model

图 3 信任链传递模型

2.5 TPM-APM可信性分析

(1) 对原系统网络的影响

对时延参数进行测量时,我们需对印制电路板的原网络增加测量引线(TPM-APM 测量模块搭接到数据总线/被测网络的走线).而测量引线是受控阻抗传输线,能做到与 TPM-APM 模块阻抗匹配.所以测量引线与 TPM-APM 模块的加入不会对原网络造成干扰.本文使用 Tektronix TDS3054B 示波器对某嵌入式系统高速 SDRAM 的信号进行眼图的实际测量,验证测量引线及 TPM-APM 模块的加入是否会影响原网络信号传输.此嵌入式系统中 SDRAM 的地址线及数据线是对信号完整性要求最高的部分,是整个印制板性能指标的关键.如果测量模块此处对 SDRAM 传输信号的影响不大,则系统中其他低速部分对信号的影响可以忽略.图 4(a)是原网络数据总线最低位的眼图,图 4(b)则是增加了 9 000 mil 的测量引线及 TPM-APM 模块(使用 TDC-GP1 芯片)后,相同位置的测量结果.如图 4 所示,在测量引线与 TPM-APM 模块阻抗匹配的情况下,TPM-APM 模块的加入对原网络信号质量没有明显的影响.



(a) 原网络 (b) 增加测量模块

Fig.4 The eye pattern of least significant bit

图 4 数据总线最低位眼图

(2) 信任机制问题

由于 TPM-APM 设计为 TPM 的子模块,封装于 TPM 芯片的内部.作为 TPM 的子模块,TPM-APM 的加入并不会引入新的信任机制问题.

3 结论与展望

本文在文献[12]研究工作的基础上进一步对 TPM-APM 子模块进行了合理的逻辑分层设计,详细阐述了以时延模拟参数为度量对象的 TPM-APM 子模块的改进设计与实现方法,并通过对眼图的实际测量比对,验证了 TPM-APM 子模块设计方案的可行性.实验结果表明,TPM-APM 子模块在不破坏原有 TPM 设计规范的前提下,从模拟量层面给出了度量可信平台硬件完整性的新途径,从而有效地解决了针对可信计算平台的物理攻击问题.本文所阐述的以时延参数为度量对象的 TPM-APM 子模块设计只是 TPM-APM 子模块的一个简单实现.如果仅通过时延来衡量可信硬件平台印制电路板的特定网络,则仍然不够全面(攻击者可以利用时延芯片来绕过检测).如何合理地选择、划分可信计算平台印制电路板的多个关键特定网络,并合理、高效、系统地测试包括阻抗特性、时延特性、功耗等一系列模拟量参数,从而构建更加完善的可信硬件平台数模结合度量体系,是下一步需要认真深入研究的内容.

References:

[1] Feng DG, Qin Y, Wang D, Chu XB. Research on Trusted Computing Technology. Journal of Computer Research and Development. 2011,48(8):1332−1349 (in Chinese with English abstract).

[2] Trusted Computing Group. TPM main part 1 design principles specification Version 1.2 (Revision 116). 2011. http://www.trustedcomputinggroup.org

[3] Trusted Computing Group. TPM main part 2 TPM structures specification Version 1.2 (Revision 116). 2011. http://www.trustedcomputinggroup.org

[4] Trusted Computing Group. TPM main part 3 commands specification Version 1.2 (Revision 116). 2011. http://www.trustedcomputinggroup.org

[5] Trusted Computing Group. TCG PC client specific TPM interface specification (TIS) Version 1.3. 2013. http://www.trustedcomputinggroup.org

[6] 沈昌祥,张焕国,冯登国,曹珍富,黄继武.信息安全综述.中国科学(E 辑:信息科学),2007,37(2):129−150. [doi: 10.3321/j.issn:1006-9275.2007.02.001]

[7] Gu WJ, Wang X, Chellappan S, Xuan D, Lai TH. Defending against search-based physical attacks in sensor networks. In: Proc. of the IEEE Int'l Conf. on Mobile Adhoc and Sensor Systems. 2005. [doi: 10.1109/MAHSS.2005.1542839]

[8] Wang X, Chellappan S, Gu WJ, Yu W, Xuan D. Policy-Driven physical attacks in sensor networks: Modeling and measurement. In: Proc. of the IEEE Int'l Conf. WCNC on Wireless Communications and Networking, Vol.10. 2006. 671−678. [doi: 10.1109/WCNC.2006.1683549]

[9] Kang WJ, Yu K, Yu GY, Zou XC. Novel security strategies for SRAM in powered-off state to resist physical attack. In: Proc. of 2009 the 12th Int'l Symp. Conf. on Integrated Circuits. 2009. 298−301.

[10] Vasudevan A, McCune J, Newsome J, Perrig A, Doorn LV. CARMA: A hardware tamper-resistant isolated execution environment on commodity x86 platforms. In: Proc. of the 7th ACM Symp. on Information, Computer and Communications Security. ACM, 2012. 48−49. [doi: 10.1145/2414456.2414484]

[11] Choi P, Kim DK. Design of security enhanced TPM chip against invasive physical attacks. In: Pavan S, Serdijn W, Chung H, eds. Proc. of the 2012 IEEE Int'l Symp. on Circuits and Systems (ISCAS). IEEE, 2012. 1787−1790. [doi: 10.1109/ISCAS.2012.6271612]

[12] Chen X, Du HT, Li GS, Ma JF. Design of TPM chip against physical attacks. Journal of Wuhan University (Natural Science Edition), 2010,56(2):143−146 (in Chinese with English abstract).

[13] Chen Y，Wu Z，Chen J, Wan WN, Lü YQ. Implementation of equivalent power consumption coding secure against side channel attack. Journal of University of Electronic Science and Technology of China, 2008,37(2):168−171 (in Chinese with English abstract). [doi: 10.3969/j.issn.1001-0548.2008.02.002]

[14] Mao J, Zhou YJ. Trusted platform module countermeasures against hardware attacks. Information Technology, 2006,30(6):27−30 (in Chinese with English abstract). [doi: 10.3969/j.issn.1009-2552.2006.06.009]

[15] Bratus S, D'Cunha N, Sparks E, Smith SW. TOCTOU, traps, and trusted computing. In: Trusted Computing-Challenges and Applications. Berlin, Heidelberg: Springer-Verlag, 2008. 14−32. [doi: 10.1007/978-3-540-68979-9_2]

[16] Sparks ER. A security assessment of trusted platform modules. Technical Report, TR2007-597, Department of Computer Science, Dartmouth College, 2007. http://www.ists.dartmouth.edu

[17] Caignet F, Delmas-Bendhia S, Sicard E. The challenge of signal integrity in deep-submicrometer CMOS technology. In: Proc. of the IEEE, 2001,89(4):556−573. [doi: 10.1109/5.920583]

[18] Brooks D. Signal Integrity Issues and Printed Circuit Board Design. Prentice Hall Professional, 2003.

[19] Kalisz J, Szplet R, Pasierbinski J, Poniecki A. Field-Programmable-Gate-Array-Based time-to-digital converter with 200-ps resolution. IEEE Trans. on Instrumentation and Measurement, 1997,46(1):51−55. [doi: 10.1109/19.552156]

[20] Acam Corporation. TDC-GP1 evaluation system datasheet. 2007. http://www.acam.de

[21] Szplet R, Kalisz J, Szymanowski R. Interpolating time counter with 100 ps resolution on a single FPGA device. IEEE Trans. on Instrumentation and Measurement, 2000,49(4):879−883. [doi: 10.1109/19.863942]

附中文参考文献:

[1] 冯登国,秦宇,汪丹,初晓博.可信计算技术研究.计算机研究与发展,2011,48(8):1332−1349.

[12] 陈曦,杜海涛,李光松,马建峰.抗物理攻击的 TPM 芯片改进设计.武汉大学学报(理学版),2010,56(2):143−146.

[13] 陈运,吴震,陈俊,万武南,吕永其.防范边信道攻击的等功耗编码实现算法.电子科技大学学报,2008,37(2):168−171. [doi: 10.3969/j.issn.1001-0548.2008.02.002]

[14] 毛健,周玉洁.可信平台芯片的一种硬件攻击防范设计.信息技术,2006,30(6):27−30. [doi: 10.3969/j.issn.1009-2552.2006.06.009]

陈曦(1984－),男,浙江绍兴人,博士,助理工程师,主要研究领域为可信计算,移动支付,移动互联网,密码学.
E-mail: cx8408@hotmail.com