

一种改进的基于故障分析的逻辑加密算法

黄一鸣¹, 冯建华^{1,2,3}, 张小飞¹

(1 北京大学 微电子学研究院, 北京 100871; 2 北京大学 软件与微电子学院, 北京 100871;
3 北京大学 (天津滨海) 新一代信息技术研究院, 天津 300450)

摘 要: 为了保护 IC 设计人员的知识产权, 本文提出了一种改进的基于故障分析的逻辑加密算法, 选择多路选择器作为密钥门电路, 并根据其工作特性改善原有的故障分析算法. 采用本方法加密后的电路与原电路输出相比可以实现更好的汉明距离. 而且, 与原故障分析方法相比, 该方法只需采用更少的密钥门即可实现目标汉明距离.

关键词: 逻辑加密; 组合逻辑电路; 密钥门; 多路选择器

中图分类号: TN43

文献标识码: A

文章编号: 1000-7180(2018)01-0001-05

An Improved Logic Encryption Algorithm Based on Fault Analysis

HUANG Yi-ming¹, FENG Jian-hua^{1,2,3}, ZHANG Xiao-fei¹

(1 Institute of Microelectronics, Peking University, Beijing 100871, China;
2 School of Software & Microelectronics, Peking University, Beijing 100871, China;
3 Beida (Binhai) Information Research, Tianjing 300450, China)

Abstract: In order to protect IC designers' s intellectual property, In this paper, an improved insertion algorithm based on fault analysis was proposed. MUXes are chosen as the key gates and insertion method is improved based on its working property. This technique achieves better Hamming Distance between the correct and the wrong outputs. Furthermore, the target of the Hamming Distance is achieved using smaller number of key-gates compared to traditional method.

Key words: logic encryption; combinational logic circuit; key gate; MUX

1 引言

随着集成电路产业的不断进步, 设计者必须自己承担起保护设计版权的任务^[1-3]. 目前行之有效的保护方法之一就是设计者通过某种方式将自己设计的电路功能隐藏起来^[4-6], 再交付给生产商. 用来保护 IC 设计的知识产权^[7].

逻辑加密是指通过向原有的设计电路中增加新的门电路作为密钥电路从而达到对原有的设计功能进行隐藏的目的, 工作原理如图 1 所示. 每一个密钥门电路都至少拥有一位的输入作为密钥. 设计者可以自行决定在电路的何种位置插入何种门电路作为密钥门. 而一旦密钥门的种类和位置固定以后, 所得

到的密钥也相应的确定下来. 整个电路只有在密钥正确的情况下才能输出正确的功能, 而正确的密钥只有设计者自己才知道, 生产商是无从获取的.

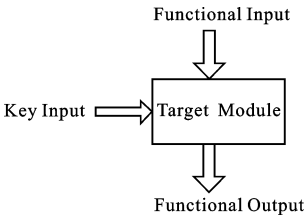
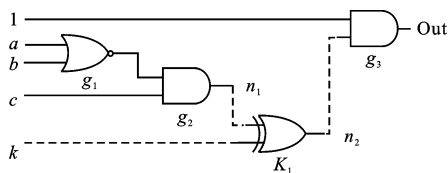


图 1 逻辑加密

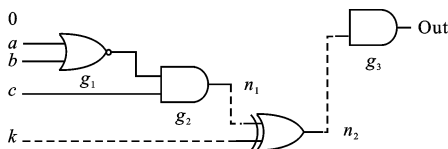
对于加密后的电路, 针对相同的输入, 当密钥错误时输出也应该是错误的. 如果在施加错误密钥的情况下还能够得到正确的输出, 或者得到的

输出是正确情况下的反码,都说明该加密方法是脆弱的.因此,只有当错误输出与正确输出有一半比特位不一致时,该加密方法才最有效,即密钥正确与错误两种情况下的输出之间存在着 50% 的汉明距离^[8].

EPIC^[7]最先提出了逻辑加密的概念,这种方法是在原电路中随机的插入密钥门以达到加密的目的.但这种基本的加密很难保证得到令人满意的加密效果.如图 2 所示, g_1, g_2 和 g_3 为原电路, K_1 为设计者插入的密钥门电路.加密后,对于密钥 k 而言正确值应该为 0. 当密钥错误时,由于异或门的作用,线 n_2 的值将会与线 n_1 的值相反,在图 2(a)中,由于 g_3 的另一个输入被置为 1,所以电路的输出将受到线 n_2 值的控制从而输出错误的结果,但是在图 2(b)中,无论输入的密钥 k 正确与否,电路的输出都会是 0. 以上的例子说明 EPIC 这种随机插入密钥门的方法具有一定的局限性.



(a) 错误密钥产生错误输出



(b) 错误密钥产生正确输出

图 2 异或门作为密钥门

自此之后,不少研究人员尝试从加密门和加密点的选择两条路径对逻辑加密方法进行改善. Dupuis 等^[9]提出了一种加密算法以减少电路中可控制性差的节点. Baumgarten 等^[10]通过向电路中插入一系列查找表(Lookup Table, LUT)取代异或门实现对电路的加密. 在文献^[11]中, Rajendran 提出了一种基于故障分析的方法选择插入点使得 50% 汉明距离的加密标准更容易达到. 在文献中,作者介绍了一种被称作故障响应的算法对电路中的节点计算相应的故障响应值,并选择最合适的点插入异或门或多路选择器. 当采用异或门作为密钥门进行加密时,这种方法效果非常显著. 但是,当密钥门为多路选择器时,该方法效果并不明显. 这是由于异或门可以保证当密钥错误时,密钥门的输出一定可以被改变,而当密钥门为多路选

择器时,如图 3 所示,由于其另一个假线的输入也是从原电路中选择,因此无法保证多路选择器真线和假线两个输入端口的值一定是不同的. 这种情况下,即使密钥错误,无论是密钥门的输出还是电路的输出都很有可能是正确的. 而异或门作为密钥门的缺点也很显著,假设攻击者通过某种方法获知该异或门为密钥门时,则正确的密钥显而易见应该为 0^[12].

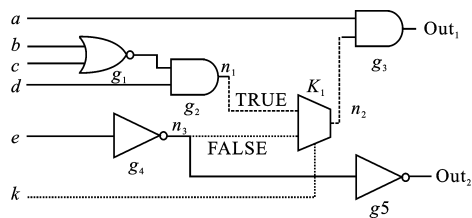


图 3 多路选择器作为密钥门

多路选择器在对于密钥的隐藏性上具有明显的优势,即攻击方即使确定密钥门也无法获得真实的密钥. 基于该特性,本文将选取多路选择器作为加密门. 在 Rajendran 的论文中,故障响应被用作决定加密门位置的唯一指标,而在计算故障响应时,并没有考虑加密门的类型. 本文将基于所选择的多路选择器提出一种对于故障响应的改进算法,该算法同时考虑了加密点的位置和多路选择器的输入特性,在保证多路选择器对密钥的隐藏性的基础上改善逻辑加密的效果.

2 故障响应算法的局限性

根据 Rajendran 的论文介绍,插入多路选择器作为加密门共需要两个步骤. 第一步,在原电路中选择应该被加密的点,并将该点作为 T 点与多路选择器的真线连接;第二步,挑选原电路中的另一点作为 F 点与多路选择器的假线进行连接.

如图 3 中电路所示,线 n_1 被作为真线与多路选择器的真端口进行相连,线 n_3 则作为假线与多路选择器相连. 而 n_1 和 n_3 的值并不能保证在所有情况下都相反,当 n_1 的值与 n_3 的值相同时,即使施加的密钥 k 错误,电路的输出也不会受到影响.

公式(1)中定义了故障响应算法,该算法被用来确定加密的 T 点,实施该算法时,根据公式定义,对电路中的每个内部节点计算相应的故障响应值并进行相互比较,故障响应值最大的内部节点即被选作与多路选择器真线端口相连. 在对节点 x 进行故障响应的计算时,首先对该点模拟固定为 0 的固定故障, NoP_0 表示向电路施加输入向量后,能够在输出

端检测到该固定故障的输入向量的个数, NoO_0 则表示该固定故障使得电路输出被改变的总位数. 相似的, NoP_1 和 NoO_1 表示对该点模拟固定为 1 的固定故障时的参数.

$$FI = NoP_0 * NoO_0 + NoP_1 * NoO_1 \quad (1)$$

确定多路选择器的真线输入后, 公式(2)定义的相反度量(Contradiction Metric)被用来确定多路选择器的假线输入. 当真线输入点确定后, 该点的 0、1 概率也被唯一确定. 对电路中其他内部节点, 分别计算其为 0 和为 1 的概率, 并计算相应的相反度量, 选择相反度量最大的假点与多路选择器的假线输入相连.

$$CM = P_{0, \text{true}} * P_{1, \text{false}} + P_{1, \text{true}} * P_{0, \text{false}} \quad (2)$$

在传统的方法中, 选择 T 点和 F 点的过程是分离的. 虽然根据 CM 可以找到相反概率最大的 T 点和 F 点, 但这并不能保证 T 点和 F 点的值相反时刚好可以对电路的输出产生影响. 为进一步说明这个问题, 表 1 根据 T 点和 F 点的值以及该 T 点发生固定故障时是否会对输出产生影响, 将输入向量分为 8 种, 每一种输入向量的数量分别为 P_1 到 P_8 , 表中第 4 行中值 1 表示 T 点发生固定故障时可以在输出端检测到, 值 0 则表示不能在输出端检测到. 如正表第一列所示, 对于某对 T 点和 F 点, 使得 T 点的值为 0, F 点的值为 0, 且 T 点若发生固定为 1 的故障时不会对输出产生影响的输入向量的数量为 P_1 , 第二列表示使得 T 点的值为 0, F 点的值为 0 且 T 点若发生固定为 1 的故障将会对输出产生影响的输入向量个数为 P_2 .

表 1 多路选择器作为密钥门时输入向量的分类

数量	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
T 点	0	0	0	0	1	1	1	1
F 点	0	0	1	1	0	0	1	1
响应输出	0	1	0	1	0	1	0	1

当针对 T 点计算故障响应(FI)时, $NoP_0 = P_6 + P_8$ 且 $NoP_1 = P_2 + P_4$. 显而易见, P_2 和 P_8 所表示的输入向量中, 尽管若 T 点产生固定故障会对输出产生影响, 但 T 点的值和 F 点的值一致. 因此若将该组下选出的 T 点和 F 点分别与多路选择器的真线假线输入相连, 由于真假线的值并没有发生改变, 即使密钥错误, 电路的输出也不会发生改变. 若更加精确的采用故障响应算法进行计算, NoP_0 应等于 P_6 , NoP_1 应等于 P_4 , NoO_0 和 NoO_1 也会相应的进一步精确. 根据以上推论, 本文提出了一种改进的故障响应算法, 同时考虑了 T 、 F 点的值以及对输出的影响

程度, 具体的计算方法将在下一章节进行详细说明.

在原作者 Rajendran 的传统算法中, 另一个较为严重的问题是在选择 F 点时并没有考虑逻辑循环的产生, 而在实际的设计过程中, 由于 F 点的选取有可能来自多路选择器输出之后的节点, 因此, F 点的值既受多路选择器输出的影响, 又同时影响多路选择器的输出, 图 4 是逻辑循环的一个简单例子. 在图中, 线 n_2 的值即为 F 点的值. 当密钥 k 错误时, 多路选择器的输出 n_1 的值即为 F , 而 n_2 与 n_1 相反, 于是进一步改变了 F 的值, 逻辑循环便由此产生. 逻辑循环的出现将会使得加密后的电路无法通过 EDA 工具进行综合, 更无法进行后续的设计.

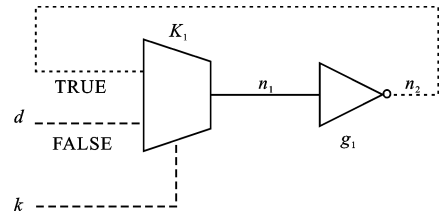


图 4 逻辑循环

3 改进的故障响应算法

首先, 为解决前文提到的逻辑循环问题, 可以采用时序型多路选择器代替原有的密钥门. 时序型多路选择器如图 5 所示, 其中, F 点并不直接与多路选择器的假线输入相连, 而是通过一个 D 触发器, 将 D 触发器的输出接入多路选择器的假线. 由于触发器会产生一个时钟周期的时延, 所以真正接入多路选择器假线的值为上一时刻 F 点的值. 该方法虽然可以有效解决逻辑循环问题, 但无法改善多路选择器的加密效果, 因此本文进一步提出了一种新故障响应算法(New Fault Impact, NFI), 采用该算法进行加密时则不能采用时序型多路选择器, 具体原因将在后文解释.

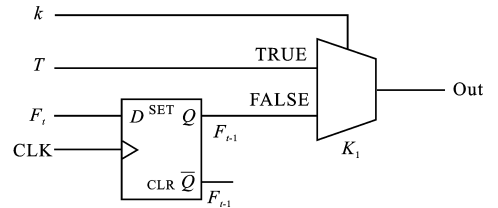


图 5 时序型多路选择器

公式(3) 定义了新的故障响应算法. 根据该算法, 每一步计算时都将 T 、 F 点的值以及是否影响输出同时考虑, 因此, 可以更加精确的计算找到相应的 T 点和 F 点.

$$NFI = NoP_0 * NoO_0 \mid_{F=0 \& F \in \epsilon(T)}$$

$$+ \text{NoP}_1 * \text{NoO}_1 \mid_{F=1 \& F \in \epsilon(T)} \quad (3)$$

原故障响应算法是针对每个内部节点计算出最适合做 T 点与多路选择器真线输入相连的点,改进的 NFI 算法是针对电路内部的节点对,假设其中一个为 T 点并模拟固定故障,另一个点为 F 点,计算每一节点对的 NFI,值最大的节点对即为最适合与多路选择器相连的 T 、 F 组合。与原算法相似, NoP_0 表示能够在输出端检测到 T 点的固定为 0 故障的输入向量个数, NoO_0 表示输出受到该故障响应的总位数。 $\mid_{F=0 \& F \in \epsilon(T)}$ 表示对 T 点模拟固定为 0 的故障,只有使得 F 点也同时为 0 且对输出产生影响的输入向量才能被计入 NoP_0 ,相应的对输出影响的位数被计算如 NoO_0 。而 F 的选择必须是在 $\epsilon(T)$ 的集合内, $\epsilon(T)$ 是受 T 点影响的一个可选的 F 点集合。当在 T 点模拟固定故障时,若电路内部另一点的值受此影响而发生改变,则该点不是 F 的可选择点,即不属于集合 $\epsilon(T)$ 。通过该方法,既可以最大程度上保证设计后的电路不会出现逻辑循环现象,又更加精确的确定了应该进行加密的 T 、 F 对。采用相似的方法即可计算 $\text{NoP}_1 * \text{NoO}_1 \mid_{F=1 \& F \in \epsilon(T)}$ 的值。

基于 NFI 算法插入多路选择器

```

Input: Netlist, KeySize, EncryptionKey
Output: EncryptedNetlist
// LocationSelection Phase
For (i=1; i<KeySize; i++)
  For each gate j∈Netlist
    For each gate k∈Netlist & k!=j & k∈
      compute NewFaultImpact for j & k pair;
    End
    now j is fixed, select k with the highest NFI to be right
  match for j;
  End
  Select the j & k pair with the highest NFI;
// Modification Phase
Insert MUX;
Connect the j as the TRUE and k as the FALSE to the
first and second wire of the MUX
Update Netlist;
Apply Test Patterns;
End
  
```

根据以上阐述可知,原故障响应算法(FI)是计算与 T 点值不同的概率最大点,从而寻找到相应的 F ,这种算法是基于统计概率的,与电路节点具体时刻的值没有必然联系,因此时序型多路选择器带来的一个时钟周期的时延不会对加密效果产生影响。而新故障响应算法(NFI)本质上是寻找与 T 点具有

一定相关性的 F 点,例如 T 和 F 受共同的输入所控制,即如图 6 所示。因此一个时钟周期的延迟将有可能对 NFI 的加密效果产生影响。这也是在 NFI 算法中必须通过采用集合 $\epsilon(T)$ 对 F 点的选择进行限制以达到避免逻辑循环的目的的重要原因。

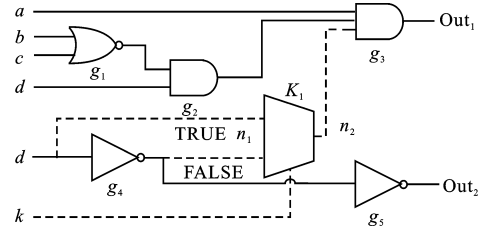


图 6 T 点与 F 点受相同输入信号控制的情况

4 实验结果

为了验证本文提出的新算法,实验中采用了 ISCAS-85 的基准电路 c499、c880、c1908、c2670、c3540。针对每一个基准电路,分别采用了三种逻辑加密方法,第一种是随机插入密钥门电路,第二种是根据 Rajendran 提出的方法 FI 插入密钥门,第三种则是本文提出的改进的算法 NFI。实验过程中采用了 VC++6.0 对每个基准电路进行修改以模拟固定故障,采用 Modelsim 10.1 进行仿真,结果如图 7、图 8、图 9 所示。其中图 7 为随机向各电路中插入不同数量的密钥门后,密钥正确和密钥错误时得到的输出之间的汉明距离,图 8 为采用原故障响应算法加密的结果,图 9 为采用改进的故障响应算法进行加密的结果。对于不同的基准电路,为达到最大汉明距离所采用的密钥门数量不尽相同。其中各电路达到最大汉明距离所必需采用的最少密钥门数量如表 2 中所列示。

表 2 达到最大汉明距离需最少采用的密钥门数量

	c499	c880	c1908	c2670	c3540
传统型	45	60	65	50	50
改进型	45	35	35	45	50

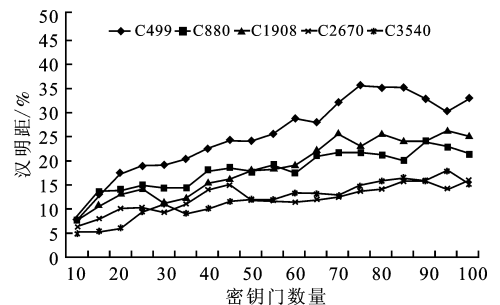


图 7 随机插入密钥门的加密效果

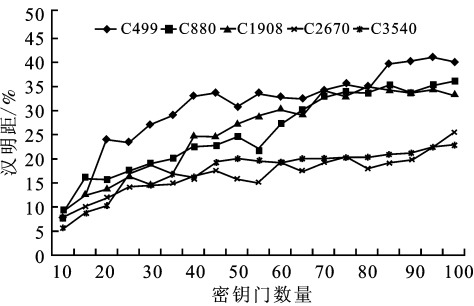


图 8 传统故障分析法插入密钥门的加密效果

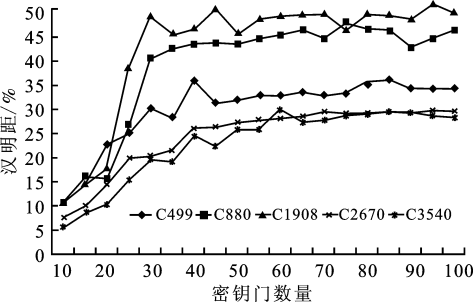


图 9 改进型故障分析法插入密钥门的加密效果

由实验结果可知,除 c499 外,本文提出的改进的算法在其他电路上应用时加密效果有显著提高.在电路 c499 中,共有 170 个内部节点,电路规模较小,不足以显示出 NFI 对于原算法的提升.经深入分析可知,其原因在于较小规模的电路中,出现表 1 中 P_2 和 P_8 所代表的输入向量的机会也相对较小,而本文提出的方法正是对以上情况作出的优化.

在此针对每个电路分别选取达到最接近 50% 汉明距离所必需采用的最少数量密钥门进行加密,并在 SMIC180 nm 工艺下对电路进行进一步仿真,得到的各电路的功耗、面积开销等情况.各电路的面积、功耗、时延情况如图 10 所示.由实验结果可知,采用改进型算法,电路各项开销均有所下降,这本质上是由于所采用的密钥门数量减少所致.

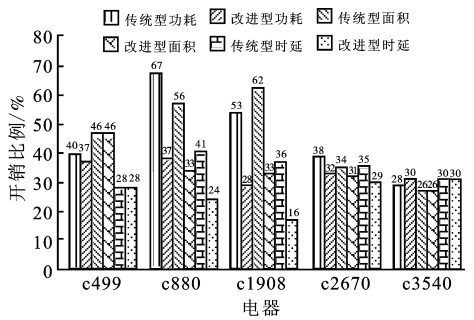


图 10 不同电路在最接近 50%汉明距时的开销

5 结束语

本文基于故障分析的逻辑加密方法,根据多路选择器的输入特性,将真线与假线的选择相结合,对原有的加密算法进行改善,同时避免了加密过程中产生逻辑循环,实验验证了改进算法的有效性.采用改进的算法进行加密,不仅可以取得更好的汉明距离,提高安全性,而且也可减小由于插入密钥门而带来的面积、功耗和延迟开销.

参考文献:

[1] Adee S. The hunt for the kill switch[J]. IEEE Spectrum, 2008, 45(5):34-39.

[2] Guin U, Dimase D, Tehranipour M. Counterfeit integrated circuits: detection, avoidance, and the challenges ahead[J]. Journal of Electronic Testing, 2014, 30(1):9-23.

[3] Torrance R, James D. The state-of-the-art in ic reverse engineering [J]. International Workshop on Cryptographic Hardware & Embedded Systems Ches', 2009(5747):363-381.

[4] Wang X, Tehranipour M, Plusquellic J. Detecting malicious inclusions in secure hardware: Challenges and solutions[C] // IEEE International Workshop on Hardware-Oriented Security and Trust. IEEE Xplore. Anaheim, CA, USA, 2008:15-19.

[5] Tehranipour M, Koushanfar F. A survey of hardware trojan taxonomy and detection[J]. IEEE Design & Test, 2010, 27(1):10-25.

[6] Malbon J, Lawson C, Davison M. The WTO agreement on trade-related aspects of intellectual property rights: A commentary[J]. IIC-International Review of Intellectual Prop, 2015, 46(8):999-1001.

[7] Roy J A, Koushanfar F, Markov I L. EPIC: ending piracy of integrated circuits[C]// Conference on Design, Automation and Test in Europe. ACM, Munich, Germany,2008:1069-1074.

[8] Rajendran J, Pino Y, Sinanoglu O, et al. Logic encryption: a fault analysis perspective[J]. IEEE Transactions on Computers, 2015, 64(2):410-424.

[9] Dupuis S, Ba P S, Natale G D, et al. A novel hardware logic encryption technique for thwarting illegal overproduction and hardware trojans[C]// On-Line Testing Symposium. Girona, Spain,IEEE, 2014:49-54.

[10] Baumgarten A, Tyagi A, Zambreno J. Preventing IC piracy using reconfigurable logic barriers[J]. IEEE Design & Test, 2010, 27(1):66-75.

三是针对磨损均衡的两级分化引入冷热数据分离策略. 将上述程序做成 module,更改 Yaffs2 对应的磨损均衡算法,并将上述文件系统 Yaffs2-Updata 移植到 mini2440 开发板中验证. 实验结果表明;仅付出 4.05%的额外擦除代价,将 NAND Flash 的寿命由 2.19 年延长到 8.23 年.

参考文献:

[1] Agrawal N, Prabhakaran V, Wobber T, et al. Design tradeoffs for SSD performance[C]// Usenix Technical Conference. Boston, Ma, Usa, DBLP, 2008;57-70.

[2] 温朝建, 严华. Yaffs2 文件系统中对 NAND Flash 磨损均衡的改进[J]. 电子技术应用, 2015, 41(6): 16-19.

[3] 杨习伟, 贺云健. 车载娱乐系统的 NandFlash 管理模式研究[J]. 单片机与嵌入式系统应用, 2008, 7(1): 19-22.

[4] Gal E, Toledo S. Algorithms and data structures for flash memories[J]. Acm Computing Surveys, 2005, 37(2):138-163.

[5] Wu M, Zwaenepoel W. eNVy: a non-volatile, main memory storage system[J]. Acm Sigops Operating Systems Review, 1994, 28(5):86-97.

[6] Lin M, Chen S. Efficient and intelligent garbage collection policy for NAND flash-based consumer electronics[J]. IEEE Transactions on Consumer Electronics, 2013, 59(3):538-543.

[7] Xu G, Wang M, Liu Y. Swap-aware garbage collection algorithm for NAND flash-based consumer electronics[J]. Consumer Electronics IEEE Transactions on, 2014, 60(1):60-65.

[8] Murugan M, Du D H C. Rejuvenator: A static wear leveling algorithm for NAND flash memory with minimized overhead[C]// IEEE, Symposium on MASS Storage Systems and Technologies. IEEE Computer Society, Washington, DC, USA, 2011;1-12.

[9] Chang Y H, Chang L P. Efficient wear leveling in NAND flash memory[M]. Inside Solid State Drives (SSDs), Springer Netherlands, 2013;233-257.

[10] Hsieh J W. Efficient on-line identification of hot data for flash-memory management[C]// Acm Symposium on Applied Computing. Proceedings of the ACM Symposium on Applied Computing. New York, NY, USA 2005;838-842.

[11] 刘柳, 黄德才. 一种逻辑块温度和物理块年龄的磨损均衡算法[J]. 计算机系统应用, 2011, 20(12): 109-113.

作者简介:

拓晶女,(1989-),硕士研究生. 研究方向为嵌入式存储系统. E-mail:13609117403@163.com.

唐磊男,(1973-),硕士,博士生导师. 研究方向为嵌入式计算机、微系统.

(上接第 5 页)

[11] Rajendran J, Zhang H, Zhang C, et al. Fault analysis-based logic encryption[J]. Computers IEEE Transactions on, 2015, 64(2):410-424.

[12] Subramanyan P, Ray S, Malik S. Evaluating the security of logic encryption algorithms[C]// IEEE International Symposium on Hardware Oriented Security and Trust. Athens, Greece, IEEE, 2015;137-143.

作者简介:

黄一鸣男,(1993-),硕士研究生. 研究方向为硬件木马及可信性设计. E-mail:ymhuang@pku.edu.cn.

冯建华男,(1964-),博士,副教授. 研究方向为数字、模拟和混合信号电路测试和可测试性设计.

张小飞男,(1991-),硕士研究生. 研究方向为硬件木马.